AD________________

Award Number: DAMD17-99-C-9001

TITLE: Defense Healthcare Information Assurance Program

PRINCIPAL INVESTIGATOR: Archie Andrews

CONTRACTING ORGANIZATION: Advanced Technology Institute
Charleston, South Carolina 29418

REPORT DATE: June 2001

TYPE OF REPORT: Final

PREPARED FOR: U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

DISTRIBUTION STATEMENT: Approved for Public Release;
Distribution Unlimited

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** June 2001	**3. REPORT TYPE AND DATES COVERED** Final (15 Oct 98 - 31 May 01)

4. TITLE AND SUBTITLE
Defense Healthcare Information Assurance Program

5. FUNDING NUMBERS
DAMD17-99-C-9001

6. AUTHOR(S)
Archie Andrews

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Advanced Technology Institute
Charleston, South Carolina 29418

E-Mail: andrews@aticorp.org

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*

This report summarizes the work of the Defense Healthcare Information Assurance Program (DHIAP) for the period, 15 October 1998 to 31 May 2001. It describes the work completed in the Phase I (research) and Phase II (tool development, testing, and analysis) program activities. In Technical Assessment, the DHIAP Team conducted Information Security Evaluations at two military medical treatment facilities and used results to develop recommendations for improving information assurance capability for MTFs in general and for the military healthcare system overall. In Prototype Development/Demonstration/Transition, the Team developed, tested, and transitioned to MTF operational use a RADIUS-compliant capability for assuring the identity of remote dial-in users of computer systems and controlling their access to those systems. In Risk Analysis, the Team developed and tested a methodology and tools for assessing risk to information assets. The methodology (both expert-led and self-directed versions) is based on the OCTAVE^{SM} Method developed by SEI. In Business Case Analysis (BCA), the Team developed a methodology for analyzing cost, operational and functional impact, and risk to the military of deploying technologies affecting healthcare information security, and exercised and refined that methodology during the course of conducting BCAs in four investigations of information assurance technologies. Technologies investigated were remote authentication of dial-in users, authentication, role-based access control, and audit of computer use and access. In Simulation Capability, the Team created and demonstrated the functional capabilities of an alpha version survivability simulator designed to assess impacts on mission survivability.

14. SUBJECT TERMS
Information Security, Information Technology, Information Assurance, RADIUS, computer Security, Risk Analysis, Business Case Analysis, Survivable Systems, Simulation

15. NUMBER OF PAGES
113

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** Unlimited

FOREWORD

Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the U.S. Army.

(X) Where copyrighted material is quoted, permission has been obtained to use such material.

(X) Where material from documents designated for limited distribution is quoted, permission has been obtained to use the material.

(X) Citations of commercial organizations and trade names in this report do not constitute an official Department of the Army endorsement or approval of the products or services of these organizations.

( ) In conducting research using animals, the investigator(s) adhered to the "Guide for the Care and Use of Laboratory Animals", prepared by the Committee on Care and Use of Laboratory Animals of the Institute of Laboratory Animal Resources , National Research Council (NIH Publication No. 86-23, Revised 1985).

( ) For the protection of human subjects, the investigator(s) have adhered to the policies of applicable Federal Law 32 CFR 219 and 45 CFR 46.

( ) In conducting research utilizing recombinant DNA technology, the investigator(s) adhered to current guidelines promulgated by the National Institute of Health.

Principal Investigator

06/30/2001
Date

TABLE OF CONTENTS

FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

1. Introduction

The Defense Healthcare Information Assurance Program (DHIAP) was a multi-year, multi-phase program to develop and apply tools and techniques that provide an evaluation of current networks and systems and address necessary doctrine, infrastructure, training, programmatic, and technology issues to improve information assurance for Department of Defense (DOD) medical treatment facilities (MTFs).

This Final Report reviews efforts of Phases I and II of the program. As depicted in **Figure 1**, the research-focused activities of Phase I provided the basis for the development and demonstration activities of Phase II. The Phase I activities began with evaluating the vulnerability of patient information in the military healthcare system and identifying the types of activity that will be required in the future to protect it. Phase I also developed recommended solutions for some of these vulnerabilities, in one case developing and transitioning to operational use a prototype technology to protect against unauthorized information access by a remote dial-in system user and in the other cases documenting with white papers the role, requirements and characteristics of three additional examples of information assurance issues affecting the military MTF. Phase II efforts focused on enhancing the Phase I methodologies so they could be used by military organizations of all types to protect their own information resources. Phase II included three areas of research: developing Risk Analysis (RA) evaluation tools/techniques and refining them by conducting risk assessments at MTFs; developing a Business Case Analysis (BCA) methodology and refining it by conducting BCAs on various techniques for assuring protection of healthcare information in the military; and developing a Simulation Capability for assessing the effect of changes in security approaches for distributed systems. The goal of the Phase II efforts was to mature these tools to a level appropriate for transition to operational entities throughout the military, from individual MTFs to headquarters and other higher echelon organizations, for ongoing use in improving the information assurance posture of the military healthcare system.

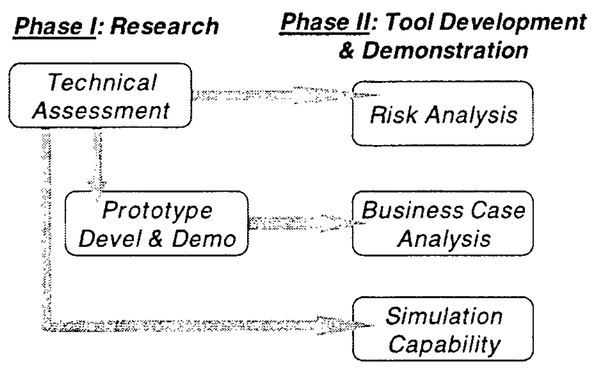


Figure 1 – Overview of Phase I – Phase II Efforts

DHIAP Phase I

Technical Assessment Task

The Technical Assessment Task was designed to evaluate installed medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities. Using a methodology developed and used by the Software Engineering Institute (SEI) called the Information Security Evaluation (ISE), DHIAP Team members experienced in system security and in healthcare operations analyzed the information protection procedures and capabilities of selected military MTFs. Upon completion of each ISE, the Team provided the site with a summary of the security issues and site security exposures that were identified, along with recommendations for improving its information security posture. When both ISEs had been completed, the Team analyzed similarities and differences in findings at the sites and prepared a "composite" report of findings and overall recommendations for improving protection of the military's healthcare information assets.

This analysis found that the security of patient information in the military medical system can be compromised and is at risk. Vulnerabilities at the local MTF level are caused, in part, by the centralized selection, administration, and maintenance of mandated health information systems. While concerted effort on implementation of current military regulatory guidance will mitigate some of the identified vulnerabilities, others that are beyond the site's capability and authority to address will require action on the part of higher echelons. Further, the military health system will face additional exposure when assessed against the emerging standards for privacy of individually identifiable health information that will be required under the pending legislation and regulatory guidance of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1]

While the goal of the Technical Assessment Task was to identify technology solutions for vulnerabilities in the military's ability to protect healthcare information, it became evident to the DHIAP Team that a multi-faceted solution is necessary. Neither technology enhancements nor carefully planned changes to current policies and procedure can alone solve current problems. Rather, as depicted in **Figure 2**, the observed state calls for an approach that encompasses policy, operations, personnel, and technology. Emphasis on any single area without regard for the other areas will not produce the desired results. Therefore, any plan to address identified information assurance issues should start with a vision of where information assurance fits into the command's policy and priorities. A comprehensive Information Assurance Policy that addresses information security in relation to operational requirements is needed to direct and guide the military's information protection activity. As policy is promulgated to the diverse organizations involved with military health information from the agencies that select and implement systems to the MTFs that treat patients, it should be used to provide a unifying influence for defining operational, personnel, and technology changes that will ensure protection of military healthcare information.

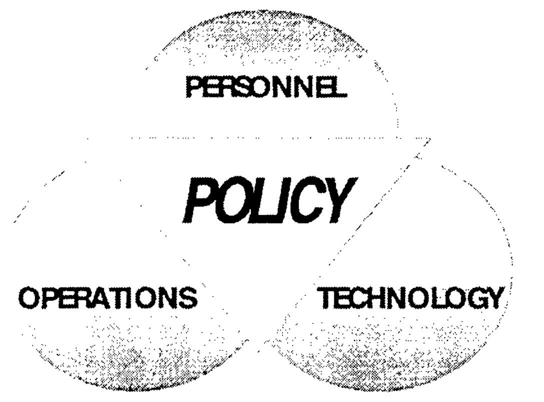


Figure 2 – Key Elements of Information Assurance

Prototype Development, Demonstration, and Transition Task

The purpose of the "Prototype" Task was to validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems, and then implement security solutions for evaluation within the

[1] *Health Insurance Portability and Accountability Act of 1996*. Public Law 104-191. August 21, 1996. URL: www.aspc.os.dhhs.gov/admnsimp/pl104191.htm.

military medical community. The DHIAP Team used findings of the Technical Assessment Task's ISEs to identify an information technology to be studied in this task and to provide the basis for the Team's design, development, and testing of a technology prototype that addressed one or more of the identified security exposures. Documented in the DHIAP proposal as three tasks, the work is presented in this report under a single heading because the work effort was highly integrated. The original task names and the work performed in each are:

- *Prototype Development* efforts (composed of Requirements Analysis, System Selection, Emerging Technology Research, System Design, and Prototype Evaluation efforts) – Produce a RADIUS-compliant[2] capability for improving information security at an MTF and across the military. In addition, conduct research and develop white papers on three other ISE-identified areas of information protection where use of technology could effect broad improvement in security of the military's patient information.
- *Demonstration* efforts – Integrate the prototype technology into an MTF's operational environment, applying it to a functional healthcare system.
- *Technology Transition* efforts – Migrate the prototype technology and associated policies and procedures to operational use in the military healthcare environment.

Based on results and lessons learned in the prototype development and demonstration activities, the Team was able to recommend policies, procedures, and methodologies required to operate the demonstration system in a secure and reliable manner. The Team successfully installed, trained, and transitioned the technology to two trial site MTFs. As a result of transition activities, the military benefited from enhanced security of healthcare information at the implemented sites, and the Team was able to develop recommendations for an approach to implementing the technology across the military healthcare system.

The DHIAP prototype effort developed and proved validity and efficiency of a number of techniques for effectively identifying and implementing new technology in a complex operational environment:

- The initial activities of the RADIUS effort and the development of the emerging technology research white papers demonstrated appropriate styles of initial, or "background," research on both the technology and the target operational environment. Because of its effectiveness, this approach was later incorporated into the Phase II *General Methodology for Business Case Analysis.*
- The RADIUS effort focused on analyzing all aspects of the technology requirements and designing the solution in relation to the requirements and the needs of its intended operational environment. (For RADIUS, this meant including circumstances particular to small, community MTFs, large regional MTFs, and regional medical command technical environments.) The ensuing design and implementation plan proved, upon deployment to the demonstration sites, to be highly appropriate to and efficient for its intended environment.
- The RADIUS effort's prototyping of the technology in a lab environment prior to rollout for operational testing led to such advantages as:

[2] Remote Authentication Dial-In Service (RADIUS)

  - Discovering and resolving most problems in a contained setting where they could be isolated more efficiently and operational entities were not affected;
  - Improving skills and knowledge of the development team within the controlled environment so impact on operational sites was minimized; and
  - Allowing the prototype configurations that were to be installed in the field to be configured and tested in the controlled lab environment so they were fully, or nearly, operational when delivered to the demonstration sites.
- RADIUS final trials in the MTF and regional operational environment allowed any remaining issues to be identified and resolved, and then permitted assessment of its performance and effectiveness in the operational setting to be evaluated prior to widespread deployment. It was the demonstration site MTFs' implementation of RADIUS that formed the basis of the Phase II pre-implementation/post-implementation Business Case Analysis of RADIUS and the BCA's recommendations for future deployment by the military.

Based on the prototype implementation experience, the DHIAP Team recommended that a broad implementation of the DHIAP RADIUS-compliant technology (i.e., multi-region or command-wide) be planned and overseen by a central coordinating authority.

Included in this task were the investigations conducted for the Emerging Technology Research. These investigations highlight important information protection issues that may impact the MTF, but addressable primarily by higher echelons. Areas of investigation were: Remote System Administration, examining the risks of external access and administration of military health systems; Public Key Infrastructure, investigating the potential application of PKI and its impact on medical organizations; and Trust Model, analyzing intentional and unintentional trust granted to users, systems, and networks.

As indicated, the results and conclusions completed in this task pointed out the importance of conducting further research into these and related areas, and this was accomplished through activities of the Phase II Business Case Analysis Task.

DHIAP Phase II

Risk Analysis Task

The Risk Analysis (RA) task's goal is to extend the principles of the Phase I ISE methodology to create and develop a risk assessment methodology for "self-directed" use directly by IT-dependant organizations. Building on ISE tools and techniques, the DHIAP Team developed an RA methodology in partnership with the Software Engineering Institute's Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM})[3] project. The methodology systematically identifies information critical assets, the elements that threaten them, and their technical vulnerabilities. The threats and vulnerabilities are used to formulate and prioritize the information security risks associated with each critical asset. Knowing the risks, the organizations are then guided through the process of developing action plans to fix the

[3] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

vulnerabilities and strategies to mitigate and/or manage the remaining risks to appropriately protect the assets.

The DHIAP Team exercised the new methodology by conducting an "expert-led" RA at an Air Force MTF. After enhancing the methodology based on knowledge gained and lessons learned during those investigations, the Team refined the methodology and tools for use as a site "self-directed" tool, trained the staff of three MTFs (two Army and one Navy) on leading the study, and mentored the MTF trainees as they prepared to lead RAs at their own sites. As part of this effort, the DHIAP Team participated in TATRC's training of Medical Information Security Readiness Teams (MISRTs), presenting the purpose and an overview of the OCTAVE Method.

Based on demonstrated success of the OCTAVE method and training conducted for the self-directed teams, the *OCTAVE Method Implementation Guide* was determined to be adequate to enable MISRTs to begin their evaluations. In terms of organizational learning, it was observed that participation in OCTAVE led to immediate insights into the organizational vulnerabilities and the need for improvements on the part of analysis team members. Some sites were able to immediately apply what they learned to improve their practices.

Business Case Analysis Task

The Business Case Analysis (BCA) task was derived to address the military's need to analyze business conditions under which it should deploy technologies for promoting health information assurance in its healthcare system. The DHIAP Team began this task by drafting a methodology for conducting BCAs on subjects that might vary from information protection technologies to processes designed to protect healthcare information. The Team worked with TATRC to select subjects to be investigated using the BCA approach, focusing on subjects that had been identified as serious information vulnerabilities during Phase I ISEs.

The first BCA topic selection was the Phase I RADIUS implementation. The goal of this BCA was to determine the effectiveness of the prototype and to assess costs of extending the implementation throughout the military medical system. The other topics were selected in light of both Phase I findings and the draft HIPAA regulatory requirements for user authentication, role based access, and audit of user access to patient information.

For each BCA, the Team adapted the methodology activities to be pertinent to the particular characteristics of the BCA subject and, upon conclusion of the investigation, produced a white paper documenting the purpose, background, analysis, conclusions, and recommendations of the investigation. As each BCA was completed, the team reevaluated and refined the BCA methodology based on lessons learned in conducting the previous investigation and additional activities or other components required due to the subject of the next investigation. A "general" BCA methodology emerged from this process, retaining characteristics specific to each of a number of different styles of investigation. The General Methodology for BCAs that evolved proved to be applicable to technologies and support processes across all stages of development and deployment, such as "what if" concepts, limited trial deployment, and fully operational deployments.

Recognizing the difference in perspective between some government agencies and the commercial world,[4] the Team developed the General Methodology for BCAs to be a tool to assist military decision-makers, one that considers a more comprehensive and applicable set of factors. The BCAs developed from application of this General Methodology are meant to address a wide range of issues. The BCA evaluation criteria consist of intangible, non-cost, operational, functional, and risk factors in addition to the traditional cost factors and economic analysis indicators. The result is a methodology that focuses on issues and forms of impact that are likely to be more relevant to the MEDCOM staff and/or MTF commander than just the cost of technology.

Simulation Capability Task

The Simulation Capability task called for the DHIAP Team to design and demonstrate a simulation capability that could be used to depict and analyze problems and solutions in mission survivability for military medical systems. This "survivability simulator" was developed to enable stakeholders to better understand the risks and consequences of potential threats, such as cyber-based attacks to medical information systems, and potentially aid in improving and protecting the integrity, confidentiality, and availability of patient records, treatment plans, and essential medical services.

The DHIAP Team built and demonstrated the alpha version of the survivability simulator, and drafted related supporting documentation (language reference manual and author style guides). The Easel simulation system holds promise as an effective research tool for fulfillment of critical mission requirements in infrastructures and other applications that must operate with incomplete information. Easel also overcomes several long-standing simulation barriers in terms of the accuracy of the simulation results and the scalability of the models and abstractions in large-scale simulations.

[4] Government organizations and military commanders, while keenly aware of cost issues, often assess cost more in terms of manpower requirements and impact on conduct of the operational mission. For an MTF commander, the dollar cost of a system is likely to be budgeted and covered by the system's program management office; the more important issues relate to subjects such as ease of deployment and transition, operational effectiveness, user acceptance, maintenance, security, etc.

2. Body

Healthcare information systems create, store, access, transfer, and exchange enormous amounts of sensitive but unclassified information. The challenge is to handle the information in ways that protect the privacy, confidentiality, and integrity of the data while still providing efficient and effective access to authorized users when and where the data is needed. The work completed in Phases I and II of DHIAP developed technologies and research reports for information protection in the military healthcare system. The methods, a discussion of the work in relation to the DHIAP statement of work, and the results of each major DHIAP task are provided below.

2.1 Technical Assessment Task

The Technical Assessment Task was designed to develop a baseline of the current state of practice of healthcare information assurance at military MTFs and provide recommendations to alleviate or eliminate identified information assurance vulnerabilities. Its major activities are depicted in **Figure 3**. The DHIAP Team applied the Information Security Evaluation (ISE) methodology that had been developed by the Software Engineering Institute's CERT Coordination Center to perform vulnerability assessments at two Army MTFs considered to be "typical" of MTFs throughout the military healthcare system. Analysis of the information gathered produced recommendations in several forms. Individually, the MTFs were given immediate feedback during technical analyses on actions they could take to address specific technical exposures, followed by a formal presentation on the state of information assurance at the site and recommendations for action to improve areas of vulnerability. Following an analysis of all vulnerabilities at the sites, a composite report was developed to provide feedback to MTF leaders and higher echelons throughout the military on systemic issues programmatic needs. Recognizing that a number of the reported issues were under control of military organizations that provided and supported systems used in the MTFs, the composite report featured recommendations for coordinated action by MTFs and other responsible agents within DOD that would improve the overall information assurance posture of the military healthcare system.

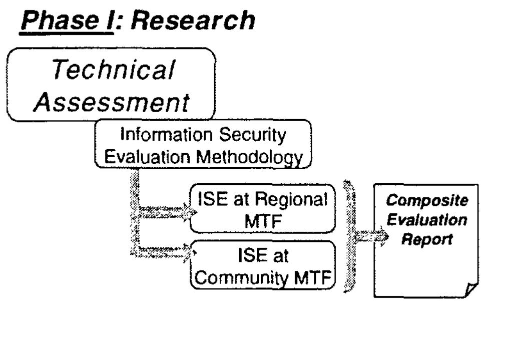


Figure 3 – Overview of Technical Assessment

Methods/Discussion:

The Technical Assessment began with two concurrent activities. In one effort, the DHIAP Team developed a Preliminary Survey questionnaire that would be used to obtain a technical and operational snapshot (summary of staff, installed systems, existing policy, current training, and current practices) of facilities being considered to participate in the task. In the other effort, TATRC nominated a number of representative sites and sent each an application package consisting of a letter outlining incentives for the nominated sites to participate in DHIAP and the Preliminary Survey. TATRC and the DHIAP Team used the sites' completed Survey information, along with input on site willingness to commit resources to the effort, to screen the sites and select the MTFs that would participate. The two MTFs selected in this way were considered to be representative of military MTFs. Because they were a Regional Medical Center

MTF and a Community Hospital MTF in the same medical region, the Team believed that the technical assessment's findings and recommendations could be generally applicable to other regions and to military MTFs overall.

Concurrent with site selection, the DHIAP Team received training from SEI in use of the ISE methodology and then prepared materials and general plan of work for performing MTF security evaluations. Once site identities were known, the DHIAP Team adapted the ISE process to be particular to circumstances at an MTF by modifying the standard ISE questionnaires to be more directly applicable to the sites' healthcare mission, and assuring that Team members with appropriate knowledge (healthcare operations, healthcare systems, technical specialties, etc.) would conduct and/or attend the appropriate interviews.

The ISE conducted at each selected MTF followed the process and general timeline depicted in **Figure 4**. In the initial site briefing, DHIAP Team leaders met with MTF leaders to define specific plans for conducting the study, determine timeframes, and establish staff commitments. The Team arranged for the site to complete a detailed Site Survey[5] that would provide additional detail about the MTF's infrastructure and operations. Upon obtaining approval of MTF leaders, the technical members of the DHIAP Team used the information as the basis for an "external probe" of MTF networks. (While the probe's purpose was to document any site-specific information available to people accessing the site from the publicly available network, the probe's scripts and activities were carefully designed to refrain from interrupting or disturbing normal operations.) The DHIAP Team used probe results in combination with Site Survey information to determine areas of emphasis for the On-Site Investigation and tailor ISE interview materials to fit the MTF's specific technical characteristics. Although the Team used the ISE methodology's standard questions to assure they covered the same set of subjects and used the same phrasing of questions at every MTF, they adjusted the sequence or emphasis of the questions that would be used in the different groups' interviews. The ISE modifications were designed to assure that (1) subjects were appropriate to the site's technology profile and interview group composition, and (2) the most critical areas of knowledge / concern appropriate for each interview group would be covered in the time allowed.

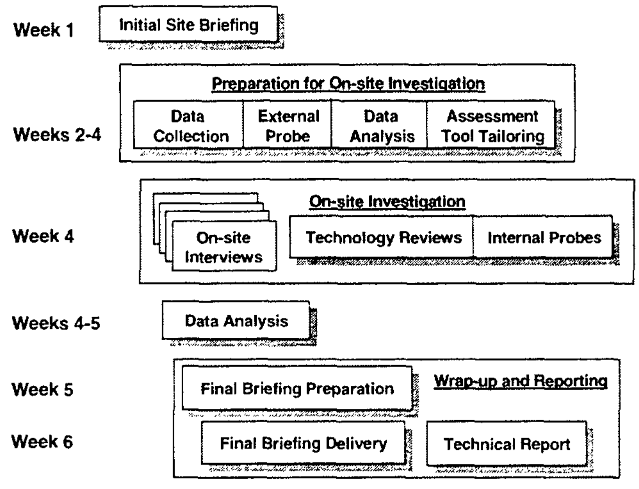


Figure 4 - ISE Activities and Timeline

[5] The Site Survey's questions had been organized to align with MTF staff responsibility areas; the requested information corresponded to subjects covered by the Preliminary Survey, but in greater detail. Questions covered such subjects as: the hardware and operating systems in use at the site; ownership, content, and support arrangements for the MTF's computer systems and network; and hardware, software, and configuration of the MTF's network.

The ISE on-site interviews gathered information on policies, practices, and an overview of the site's technical characteristics. Interview topics included organizational climate (for security), security of patient information, security policy and procedure, staff support of the security policies and procedures, external access to systems and applications, various systems administration subjects, security training, disaster recovery and backup procedure, and physical site security. In addition to interviews, the Team conducted an "internal probe" of the MTF network and machines to obtain technical information that was not obtainable in an interview. As the Team's probes identified technical vulnerabilities that were under the control of the MTF to address, they provided the information to the site's technical staff immediately and offered recommendations for addressing them. Upon completion of on-site work, the Team analyzed the collected data, grouped their observations according to the ISE's observation and evaluation categories, and developed action recommendations for addressing the core security vulnerabilities.

At the conclusion of an ISE, the DHIAP Team provided several forms of feedback to the site. Observations about certain technical issues, along with recommendations for addressing them, were provided to appropriate MTF staff during the course of the evaluation as "over the shoulder" training and on the spot recommendations for corrective action. The Team developed and delivered a Site Vulnerability Assessment Final Briefing outlining the Team's observations and recommendations for instances where site information was found vulnerable due to organizational, policy, personal, or technology issues. The briefing provided MTF leadership, the MTF's Chief Information Officer (CIO), selected staff of the Information Management group of the MTF, and all MTF staff members who had participated in the ISE process with results and recommendations of the site's evaluation. Following the briefing, the Team gave a Technical Report to the CIO that provided vulnerability details that would be helpful to the MTF's system and network administrators.

To extend the task's problem-based site recommendations to system-wide, management-focused considerations for embracing an information security culture, the Team analyzed the observations and action recommendations resulting from the two ISEs in a different way. They reclassified the recommendations according to such generally recognized management responsibility areas as policy definition, procedure definition, information protection oversight, etc. In contrast to the findings presented to the MTF sites that had emphasized specific vulnerabilities found at the MTFs and required both local action and requests to outside organizations to adequately address, the management recommendations provided as assessment of operational issues that could only be addressed through action by management at the sites and through the command authorities. These recommendations pointed out the fact that an environment exists that can either be made secure at the local level or left exposed because of the unresolved external dependencies. The associated security risk is caused by organizational structure and overall approach to distributing and supporting medical information systems and will require management recognition of the inherent weaknesses and management action throughout the medical command structure to resolve.

Results:

Detailed reports covering the individual site ISE observations and recommendations were given to MTF leaders and staff following completion of the site's ISE to help them in improving the site's information protection posture. In addition, the *DHIAP Phase I Composite Evaluation*

Report, ATI IPS TR 00-02 [CER], provided an analysis of vulnerabilities that could be common to many MTF sites and recommendations for both site-level and higher echelon action.

The DHIAP Team found that many of the identified vulnerabilities could not be fully addressed at the local level. This general conclusion was confirmed by the sites' feedback during the Site Final Briefings of observations/recommendations. [CER] describes why higher-level action, by external Command and within the MTF, is required to establish commitment, provide resources, and/or assure the oversight that is needed for mediation of many reported vulnerabilities. The Team determined that there is a need at both MTF and higher echelon levels to perform the following activities in order to establish a strong information protection culture throughout military medicine:

- Assure there is management oversight of implemented information protection capabilities and the emergence of new vulnerabilities;
- Refine and promulgate policy to foster an information protection culture;
- Use technology standards to enable certain security measures and monitor their effectiveness;
- Refine or develop clear procedures and staff training to assure that the people at every organizational level perform their work in approved ways and are equipped to make proper decisions in the course of their daily work;
- Establish appropriate organizational responsibility for the security function at the MTF level and in the higher echelons; and
- Select and properly apply appropriate technology to serve the information protection mission.

2.2 Prototype Development, Demonstration, and Transition Tasks

The purpose of the Prototype Technology Tasks was to demonstrate techniques for studying and implementing technical and operational improvements to ensure the integrity and security of the military's healthcare information. Subjects that might be addressed in this effort were drawn from the results of the Technical Assessment Task's evaluation of medical information systems and their operational environments at military MTFs, which indicated many areas where application of technology could lead to meaningful improvement in healthcare information assurance.

As depicted in **Figure 5**, the DHIAP Team used ISE results to identify specific situations where application of technology could reduce or even resolve significant exposures. To determine the subject that would be addressed in this task, they identified the more critical vulnerabilities that could be addressed with implementation of technology at an MTF, worked with MTF representatives to determine what would be most useful to them in their current state, and proposed the preferred subjects to TATRC and MTF leadership for approval. The resulting Prototype Tasks effort consisted of two elements:

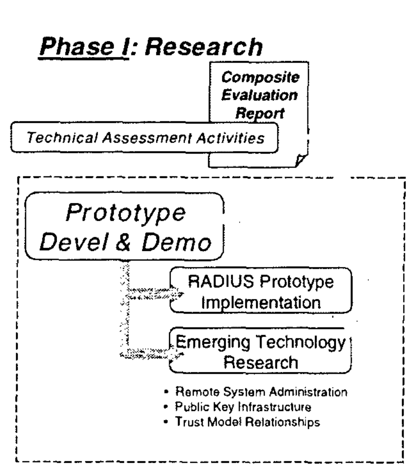

Phase I: Research
Composite Evaluation Report
Technical Assessment Activities
Prototype Devel & Demo
RADIUS Prototype Implementation
Emerging Technology Research
• Remote System Administration
• Public Key Infrastructure
• Trust Model Relationships

Figure 5 – Overview of Prototype Tasks

- Development, demonstration, and transition to operational capability at two trial site MTFs a prototype technology to address the military's mandate to comply with the Remote Authentication Dial-In User Service[6] (RADIUS) standard; and
- White papers containing technology and procedural recommendations for additional topics that the trial sites, the DHIAP team, and TATRC considered important to investigate, in order to describe and provide direction for dealing with other high priority information assurance vulnerabilities.

Methods/Discussion:

Prototype Selection and Design

The DHIAP Team began this effort by prioritizing the ISE-identified vulnerabilities using the following criteria: relevance to MTF needs, relevance to TATRC mission, MTF authority to direct and implement change, cost, complexity, and existence of a technical solution. The prioritization was also influenced by the Team's opinion of how best to make a difference in information security at the MTF. With the higher priority vulnerabilities identified, the Team researched technology development efforts that would address them and discussed their findings and preliminary conclusions with technical staff of the sites that had participated in the ISEs and TATRC.

The Team's initial recommendation was to secure e-mail service using secure socket layer (SSL) sessions so that information in transit between the remote users and the MTF computing environment would be protected. MTF staff responded that they had already begun to implement SSL for electronic mail and suggested, as an alternative, their need for technical assistance to comply with the military's directive[7] to implement RADIUS. Use of RADIUS-compliant technology would provide the MTFs with improved identification, control, and auditing of remote users who access hospital systems via dial-in.

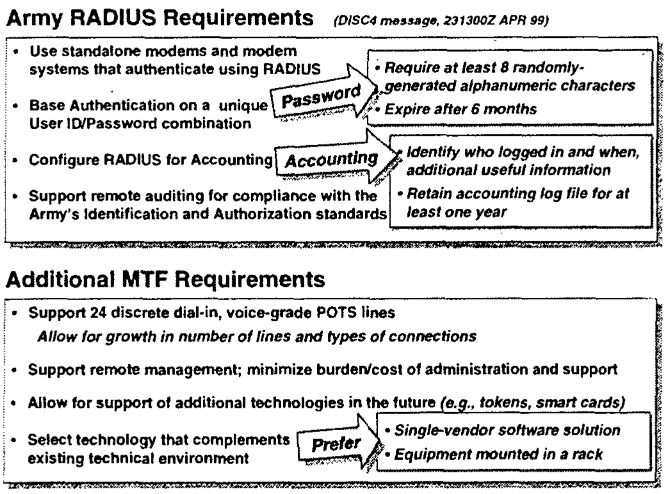
MTF staff, TATRC, and the DHIAP Team agreed to the MTF recommendation, concluding that the DHIAP Prototype Demonstration would be implementation of a RADIUS-compliant server capability fulfilling the military's requirement for identification and authentication of dial-in users. To make the RADIUS demonstration more meaningful, they arranged for the implementation to involve both a regional medical center and an associated community-level MTF so that testing and trials of the technology would include both local and cross-facility communications.

The Team designed the prototype based on technical security requirements outlined in the military's RADIUS guidance and requirements outlined in the Internet Engineering Task Force (IETF) specification of the RADIUS standard. They enhanced the design with the MTFs' operational requirements and preferences which included: compatibility with the MTFs' existing systems, support for browser-based administration, support for remote auditing, support for

[6] RADIUS is an Internet standard protocol "for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server." (Source: Internet Engineering Task Force (IETF) Network Working Group document; URL for the IETF RADIUS standard (rfc 2138) is http://www.ietf.org/rfc/rfc2138.txt.)

[7] HQ DA, DISC4, Washington DC message, subject: Network Security Improvement Program (NSIP) - Army Dial-in Standards and Policy, dtg 231300Z April 1999.

growth in the number of lines and types of communications, and minimizing the MTFs' cost of follow-on support. **Figure 6** summarizes the military's requirements for RADIUS implementation and the requirements added by the MTFs.



Army RADIUS Requirements *(DISC4 message, 231300Z APR 99)*

- Use standalone modems and modem systems that authenticate using RADIUS
- Base Authentication on a unique User ID/Password combination

Password

- *Require at least 8 randomly-generated alphanumeric characters*
- *Expire after 6 months*

- Configure RADIUS for Accounting
- Support remote auditing for compliance with the Army's Identification and Authorization standards

Accounting

- *Identify who logged in and when, additional useful information*
- *Retain accounting log file for at least one year*

Additional MTF Requirements

- Support 24 discrete dial-in, voice-grade POTS lines
  Allow for growth in number of lines and types of connections
- Support remote management; minimize burden/cost of administration and support
- Allow for support of additional technologies in the future *(e.g., tokens, smart cards)*
- Select technology that complements existing technical environment

Prefer

- *Single-vendor software solution*
- *Equipment mounted in a rack*

Figure 6 - Army and MTF Requirements for the DHIAP Prototype

The Team searched the marketplace for compliant components and evaluated alternatives against the requirements and MTF-provided selection criteria. Based on evaluation of the capabilities of the compliant components, knowledge of the level of technical skill typically available within the MTFs' Information Management Divisions, awareness of components already in place at the MTFs, and their own personal experience in using many of the candidate tools, the Team recommended that the technical solution for the RADIUS prototype be the Cisco 3600 series router with an Intel-based computer running Windows NT Server and Cisco Secure software.

Emerging Technology Research

The DHIAP Team used findings of the Technology Assessment Task ISEs as the basis for identifying certain MTF problem areas whose solutions were out of the direct control of individual sites but were important to investigate for improving the level of protection afforded patient healthcare information in the military. Initial work involved building a set of candidate requirements based on analysis of the vulnerabilities identified during the Technical Assessment task. These requirements were further refined during a requirements-gathering effort conducted by representatives of the DHIAP Team. Based on the ISE findings and knowledge of emerging technology and policies, the DHIAP Team proposed three areas of research pertinent to the security issues facing the MTFs immediately or in the near future: Remote System Administration, Public Key Infrastructure, and Trust Model Development.

With TATRC's concurrence on the subjects of investigation, the Team proceeded to investigate characteristics of the problem and develop recommendations for the types of technology, policy enhancement, and daily practice that would mitigate the identified vulnerabilities. Individuals with extensive experience in each field were assigned as lead for each report. To gather information, the DHIAP authors conducted searches of related literature (including books, articles, military regulations, and web-based articles) and worked with their professional counterparts. In addition, they made extensive use of knowledge gained from participating in interviews of the Technical Assessment Task's ISEs.

Prototype Development and Evaluation

The DHIAP Team constructed prototype systems and installed them for initial testing in two geographically separated laboratory environments. The lab installations gave the system developers and component vendors the opportunity to test all the system options and to make configuration recommendations prior to installing the systems in an operational environment. In addition, they provided the Team with experience in resolving situations that were likely to arise when the systems were installed at the trial sites. While laboratory testing allowed the Team to evaluate the suitability of the system relative to design requirements, Team members from the SEI informally evaluated the prototype's design and configuration recommendations for fit to the stated requirements and the impact on enhanced security. Both evaluations concluded that the proposed prototype met the requirements.

Demonstration

The Team used the multi-site lab environment to demonstrate the prototype's capabilities to TATRC and technical staff from the trial sites, successfully validating and verifying the prototype's capabilities for authentication, authorization, and accounting of remote access dial-in users. The demonstration provided the sites with an understanding of equipment capabilities and led to their agreement to install an Initial Operational Capability (IOC) at their sites. The systems were installed at the sites shortly following the laboratory demonstration, and the MTFs were provided with an IOC as an opportunity to become familiar with system operation, demonstrate operational effectiveness for the site's needs, plan for operational procedures, and plan for migrating their user population to the new capability.

Technology Transition

As part of the IOC, the DHIAP Team trained MTF staff on procedures for installation, configuration, operation, and maintenance of the system. In addition, the Team reviewed the sites' policy and procedures for support of secure system operations. MTF staff operated the RADIUS-compliant systems, configured their remote dial-in users, produced local user guidance, and monitored the remote users' activity in accessing MTF systems. Soon after implementation, the sites transitioned the DHIAP RADIUS-compliant system from testing to Full Operational Capability. The DHIAP Team combined the lessons learned in laboratory testing, installation, and site demonstration with the sites' feedback on their operational experience with the technology to develop a specialized technical support manual for the sites. They also used information gathered from the sites as the source of recommendations for the military's future enhancement of the DHIAP RADIUS prototype and its related policies and procedures.

Results:

MTF trials of the prototype RADIUS-compliant technology proved it to be highly suitable for use at the trial sites. A complete report on the DHIAP RADIUS architecture, including alternative strategies for implementing RADIUS in a cost-effective configuration across larger numbers of sites such as medical regions, is contained in the *Phase I Technology Demonstration Report: Prototype for Remote Authentication Dial-In User Service (RADIUS)*, ATI IPT Technical Report 00-04 [TDR]. The Team's technical documentation for installation and setup of the RADIUS prototype, developed during and after the MTF trials of the technology, is provided in the *DHIAP RADIUS Supplemental Installation and Maintenance Guide*, ATI IPT Special Report 00-03 [IMG].

The architecture and components of the prototype developed for the DHIAP RADIUS demonstration meets military requirements for modem dial-in standards and policy (which requires the RADIUS standard for implementing authentication, authorization, and accounting). The DHIAP RADIUS-compliant prototype is designed to meet RADIUS standards. It assures that the remote dial-in users who request access to the MTF network and other military network resources are who they claim to be and are granted access only to resources approved for their use by dial-in, and it assures that access by the remote user may be logged to a RADIUS-compliant accounting log.

Information Management (IM) staff at the MTF and medical region levels had expressed "local" preferences for the prototype technology's hardware/software features and support requirements. The configuration selected by DHIAP for the RADIUS-compliant system will support the local requests by providing the additional site-support features summarized in **Table 1**.

Type	Feature
System Administration	▪ Maintenance overhead is reduced by use of hardware and software common in SERMC: Windows NT Server software, Cisco Router, and Cisco IOS software ▪ Administrative burden is reduced by authenticating users against SERMC's existing Windows NT Domain Name/Password database ▪ Local and remote network administration are supported by the browser interface
Flexibility/ Extensibility	▪ Support for the expansion of security features through use of third-party token-card servers (SecurID, Enigma Logic, SecureNet, and any hexadecimal X.909 devices) ▪ Support for time-of-day access control, providing day, time and duration control ▪ Support for 10BaseT and 100BaseT network connections ▪ Scalable implementations to support clinic, hospital and region locations ▪ Support for interconnected multi-site implementations ▪ Support for minimum configurations at smaller sites ▪ Support for redundancy through network connectivity

Table 1 - MTF-Requested Features of the DHIAP RADIUS-Compliant System

Without limiting the technology's expandability and scalability, the Team's success in satisfying MTF staffs' local preferences allowed the them to minimize the amount of additional hardware, software, and training necessary to support the RADIUS-compliant system. Implementing the DHIAP technology is a matter of installing and configuring its commercial off-the-shelf tools, and, as with all technology installation, staff members' ability to apply related experience generally reduces the time and complexity of the task. By selecting components that were closely related to the products already installed in the MTFs, the DHIAP Team was able to take advantage of the MTF IM staffs' existing technical expertise. From the remote user's viewpoint, dial-in processes and procedures under the RADIUS-compliant approach are similar to methods used in the past. Once dial-in connection is established, the user's remote viewing and operation of the accessed systems is very similar to the experience at the work location. An important difference that is evident to the user occurs when RADIUS denies remote access to a system (e.g., one containing patient information) that the user may be permitted to access locally.

The Emerging Technology Research Reports outline particular information assurance issues faced within DOD that are of significant importance to protection of patient information at the military's MTF sites, as described below:

- *Remote System Administration: Issues and Recommendations*, ATI IPT Special Report 00-05 [RSA]

  This paper evaluates remote system administration in terms of DOD's actual practices, inter-agency relationships, and existing policies. It describes changes in policies and practices that would be effective for improving MTF control over external administrators, minimizing exposure of administrators' communications, and reducing exposure of other local systems if the remotely administered system should be compromised.

- *Public Key Infrastructure: Resources, Requirements, and Recommendations*, ATI IPT Special Report 00-06 [PKI]

  This paper studies current PKI implementations in both the government and private industry in terms of its components and the security requirements for those components. In defining the general issues related to PKI deployment, it notes issues that are peculiar to the MTF environment. Finally, the paper assesses the impact of PKI deployment and provides recommendations for initiation of a PKI pilot program in the DOD medical arena.

- *Trust Model: Defining and Applying Generic Trust Relationships in a Networked Computing Environment*, ATI IPT Special Report 00-07 [TRU]

  The paper describes a trust model as a tool that helps one visualize and understand the degree of confidence that is intentionally or unintentionally granted to computer users, systems, and networks based on an understanding of associated risks that are inherent with granting this confidence. It explains how an organization gains greater awareness of threats, vulnerabilities, and the risks associated with those threats and vulnerabilities. The paper concludes that knowledge of risks allows an organization to assess each risk, determine the cost, resource availability, and/or technology for mitigating each risk, and decide whether to implement a solution to mitigate the risk or accept the risk.

2.3 Risk Analysis Task

Where the ISE provided essential insight in to existing vulnerabilities in policy, procedures and technologies, it was apparent that the technique was not cost or time effective for application at every MTF. It was also apparent that a technique that could be administered by the sites would promote understanding and internalization of the results at each of the sites. MTFs need a better way of understanding their information risks and creating strategies for addressing those risks. A systematic approach to assessing information security risks and developing an appropriate protection strategy (such as the methodology developed as part of the Risk Analysis Task) can be a major component of an effective information security program. By adopting a systematic approach, an MTF can better understand its current security posture and use it to establish a benchmark for improvement. As indicated in **Figure 7**, the Phase II Risk Analysis effort leverages the knowledge gained by the DHIAP Team from developing and delivering Phase I ISEs with the SEI's prior experience in risk management for software engineering projects to develop and demonstrate an approach to Risk Analysis that can be conducted and maintained by individual sites. Consistency of the method's execution across the many sites and collection of the information for composite analysis will, as demonstrated in Phase I ISEs, allow for appropriate information to flow to higher echelons for identifying and addressing vulnerabilities that may be systemic to the military healthcare environment.

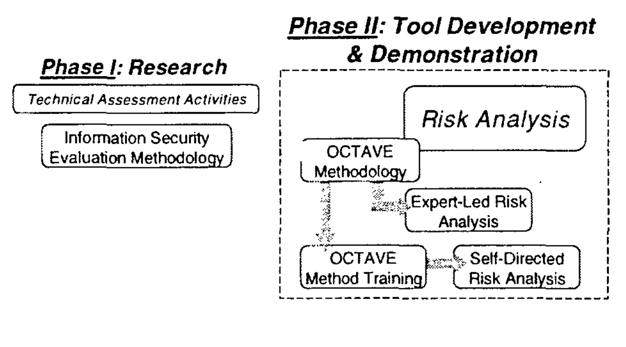

Phase I: Research
Technical Assessment Activities
Information Security Evaluation Methodology
Phase II: Tool Development & Demonstration
Risk Analysis
OCTAVE Methodology
Expert-Led Risk Analysis
OCTAVE Method Training
Self-Directed Risk Analysis

Figure 7 – Overview of Risk Analysis

2.3.1 Design/Develop OCTAVE Tools and Methodology

Methods/Discussion:

The basis of this effort was the SEI's OCTAVE risk assessment methodology. In the initial methodology development activities, risk identification and assessment techniques were integrated with the ISE methodology to create an information security risk evaluation known as "Operationally Critical Threats, Assets, and Vulnerability Evaluation" or OCTAVE. The aim was to develop a technique that could be directed by the site. Direction implies that all the expertise need not be present at the site but the site will own the management and results. In DHIAP, the Team developed and refined the OCTAVE methodology and its associated tools (templates and worksheets) for identifying and managing information security risks. **Figure 8** is a generalization of the series of workshops conducted in an OCTAVE risk assessment. Each workshop is managed by internal MTF assets and attended by MTF staff and external specialists with knowledge appropriate to meeting the goals of the session. The first series of workshops gathers the Organizational View of the security environment, supporting identification of information assets important to the mission of the organization, threats to those assets, and vulnerabilities that may expose the assets to threats. The second set of workshops document the Technological View of the environment, and the third set performs the analysis, organizing the processes of prioritizing the information assets and developing strategies for protecting them.

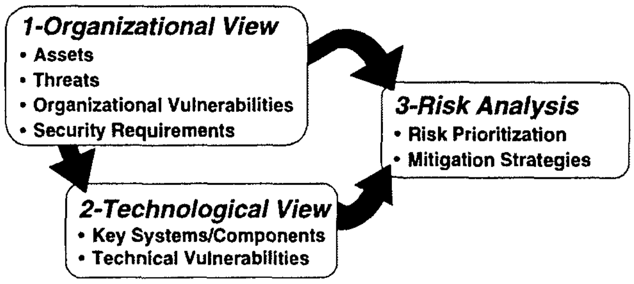


Figure 8 –OCTAVE Workshops

To identify strengths and weaknesses of both the methodology and the approach to executing it in an operational environment, the DHIAP Team tested the prototype OCTAVE methodology in an "expert-led" risk assessment at an Air Force MTF that relied on IT support from a Navy regional medical center. In this effort, the DHIAP Team led the OCTAVE workshops and provided direct support as needed to the MTF staff participating in the effort.

Based on lessons learned from the expert-led trial of the methodology, the DHIAP Team refined various components of the approach and the tools, and then began to develop materials to support site representatives in performing the risk evaluation without outside leadership (i.e., in "self-directed" mode). This enhancement of OCTAVE was closely coordinated with development of the OCTAVE training course (see Section 2.3.5 Develop/Deliver SDRA Training), producing a manual that fully documented the OCTAVE Method. The manual includes all materials needed to understand the meaning of each workshop, to lead it, to conduct its presentations, to document the information that the workshop is designed to elicit, and to perform the analysis activities that may precede or follow the workshop.

Results:

The *OCTAVE Method Implementation Guide, Version 1.0* [OCM], was published in January 2001 as the DHIAP guideline for conducting an OCTAVE self-directed risk assessment. The methodology is designed to support an organization's managing and directing the risk assessment process for itself, using internal MTF staff to perform the risk assessments tasks. This does not mean that the MTF must perform all activities internally. As a normal part of planning and conducting the assessment, leaders of the site's risk assessment effort determine if and when they need to draw upon external resources to perform certain activities of the assessment. (This might occur if the site does not have staff with the skills required to perform the activity, or if site staff cannot spare time to do the activity.) Even when external resources are included in the plan, site leaders continue to direct all risk assessment activities whether conducted by internal staff or by the external resources.

The prototype methodology was determined by TATRC and the DHIAP Team to be suitable for use by individuals experienced in conducting risk analyses to accomplish risk assessment in a complex healthcare environment (community clinics/hospital MTF site). The [OCM] incorporates for its users both the materials used in workshops of the earlier expert-led risk analysis and extensive guidance on how to conduct all workshop activities of the risk analysis, so that a team leader with no prior risk analysis experience could efficiently lead a meaningful risk analysis investigation.

2.3.2 Recruit/Select Sites for OCTAVE-based Risk Assessment

Methods/Discussion:

Concurrent with methodology development, TATRC and DHIAP Team leaders identified and recruited MTF sites to participate in four risk evaluations planned for DHIAP Phase II. Facilities of differing sizes and from each branch of the military service were targeted for inclusion among the participating MTF sites.

- One site was to conduct risk analyses led by the DHIAP Team. (The study was referred to as "expert-led," meaning that MTF staff would be guided through execution of each step of the risk analysis process by DHIAP Team members experienced in leading and executing these investigations.)
- Three additional sites were recruited for "self-directed" risk analyses, with DHIAP-trained MTF staff executing the process themselves, obtaining outside assistance to provide any needed expertise the site did not have on staff.

Results:

Four sites representative of each service and different size installations were recruited to participate in the DHIAP Risk Analyses. Execution of the initial "expert-led" risk evaluation was evaluated as smooth, efficient, and relatively unobtrusive to the site. Based on the early positive results from this first effort, it was decided to compress the testing and proceed directly to the "self-directed" risk analyses at the remaining three sites. As of the date of completion of the technical work for this contract, all sites had been trained in the OCTAVE methodology and one site was well on its way to completing its self-directed assessment.

2.3.3 Conduct DHIAP-Led Risk Assessment

Methods/Discussion:

Between September 25 and November 14, 2000, the DHIAP Team worked with senior and operational staff of the pilot site to conduct an expert-led risk analysis at the site. A total of nine briefings and workshops were held. The site's "Analysis Team" (the MTF AT), the core group with ongoing responsibility for coordinating and participating in the study, included staff from patient administration, a clinic, and the information management; other individuals from diverse areas and at all levels in the organization participated in the various workshops.

At the start of the process, the DHIAP-led MTF AT gathered input from senior management, operational management, and operational and information management staff on the facility's major information assets and identified for each asset their concerns, security requirements, and current protection strategies. Next, the Team integrated and refined the information they had gathered, identified the assets that were most critical to the facility, and moved on to identifying threats and security requirements for the critical assets. Working again with the information management staff, the Team identified the key infrastructure components that were associated with the facility's critical assets. They performed vulnerability scans on certain information assets, and obtained additional vulnerability scan results from the Base Communications Squadron, and then used the information in their assessment of technical vulnerabilities of the critical assets.

All information gathered, the Team analyzed and evaluated risks to their critical assets, developed mitigation plans for those risks, developed an organization-wide protection strategy, and defined a set of short-term action items. They reviewed plans and strategy with senior management and refined them as needed, and then began their implementation of these plans.

Results:

OCTAVE^{SM} Final Report, provided to the site and TATRC, summarizes the process followed and documents the results obtained in the expert-led risk assessment. Site personnel identified the following as their most critical information assets: medical records, personal computers, the Composite Health Care System (CHCS), the technical support they receive from the Base Communications Squadron, and the Ambulatory Data System (ADS). Major types of threats to these assets addressed in the protection plan for each asset included: human actors using network access, human actors using physical access, system problems, and "other" problems. Emphasis was placed on the need to recognize, resist, and recover from threats. An important byproduct of the risk evaluation effort and the vulnerability assessments on several key system components was identification of certain action items that the team addressed immediately.

The MTF's senior and operational staff members expressed great interest in the OCTAVE risk analysis process, and were eager to learn and continue working with the results. The workshop processes conducted at the MTF had appropriate representation by site staff, were executed smoothly, and elicited valuable information regarding the MTF site for each succeeding workshop's process. There were a number of situations where MTF staff took ownership of the material and worked extensively in the absence of the DHIAP Team experts in order to assure they were developing meaningful, accurate input to the risk analysis process. The DHIAP Team was able to capture a number of "lessons learned" from their involvement in conducting and participating in the workshops, capturing the material in a format useful for improving the OCTAVE methodology and its tools and for migrating the OCTAVE process from its "expert-led" orientation to the "self-directed" approach that would be required later in the project.

2.3.4 Develop/Deliver SDRA Tutorial

Methods/Discussion:

In order to support TATRC's one-day seminars to Medical Information Security Readiness Teams (MISRTs) to heighten Tri-service MTFs' awareness of information protection requirements and capabilities, TATRC and the DHIAP Team documented in Version 4 of the DHIAP Technical Development Plan their agreement to add this new task to program scope. The DHIAP Team agreed to develop and then present a half-day tutorial on the OCTAVE methodology at the initial sessions of TATRC's MISRT Seminars. Leaders of the Risk Analysis effort presented the tutorial at the following regional MISRT Training Seminars:

▪ Bethesda, MD	26 January 2001
▪ Chesapeake, VA	29 January 2001
▪ Biloxi, MS	5 February 2001
▪ San Antonio, TX	12 February 2001

Upon completion of these sessions, the DHIAP Team provided TATRC representatives with the tutorial materials and sufficient support to allow TATRC personnel to deliver the tutorial at the remaining MISRT seminars.

Results:

DHIAP Team members participated in providing MISRT representatives with the training endorsed by the Surgeons General of Army, Navy, and Air Force. At the same time, in a train-the-trainer mode, the DHIAP Team transferred to TATRC the knowledge and experience necessary for TATRC to assume responsibility for delivering OCTAVE methodology awareness training in the remaining MISRT training sessions.

Relative to planned DHIAP Phase II activities, the seminar's success in relaying the importance of exercising good security practice and protecting the privacy of patient health information resulted in heightened interest in the subject on the part of the participating MTF and increased their determination to participate in the upcoming OCTAVE training.

2.3.5 Develop/Deliver SDRA Training

Methods/Discussion:

In conjunction with and as a result of the experience gained during the DHIAP Team-led risk assessments, the DHIAP Team developed training designed to enable MTF staff members (the MISRTs) to execute the OCTAVE methodology as a "self-directed" (vs. "expert-led) risk assessment process. The [OCM] developed to document the OCTAVE methodology was designed to also serve as the student manual for the OCTAVE self-directed risk analysis (SDRA) training. Its contents were supplemented with focused guidance on how to use certain materials in the [OCM] during OCTAVE workshops and on how to conduct the OCTAVE SDRA training course.

Upon commitment to participate in OCTAVE SDRA training, TATRC and DHIAP Team leaders worked with MTF staff to arrange for the training course to be conducted 14-16 February 2001. Arrangements were made for MISRTs from other sites to participate in the training.

Results:

The training course was conducted on 14-16 February 2001. In addition, one group of military service representatives attended the session as observers, and TATRC and ATI DHIAP Team members participated as observers/support. For completing the training exercises, DHIAP Team trainers arranged for MISRTs from each site to work together, joined by one TATRC representative and one DHIAP Team member. Training followed the approach outlined in [OCM].

Upon conclusion of the course, participants agreed that the training, and the OCTAVE methodology that it covered, were both excellent. They all emphasized the importance of the discoveries they had made about their own sites' information processing issues as a result of completing the class exercises in their small MISRT groups, and said that the experience had made them eager to tell senior management at their sites what they had learned in such a short time and encourage scheduling and conduct of a full OCTAVE method risk assessment to occur as soon as possible.

2.3.6 Mentor SDRA at Two MTFs

Methods/Discussion:

Two sites elected to use their 26 March 2001 regional MISRT training (see Section 2.3.4 Develop/Deliver SCRA Tutorial) as the kickoff for planning their sites' risk evaluation activity because senior staff at the regional medical center and the community hospitals would learn at that meeting the importance of good security practice and the availability of the OCTAVE methodology for assessing site standing relative to good security practice. The MISRT training was well received, and the MISRTs proceeded to plan with their senior staff for a near-term start of their risk assessment efforts.

One of the site's initial schedule called for senior management briefings during February-March 2001, start of OCTAVE workshops in early April, and wrap-up activities in late June. Another of the MISRT planned to begin their OCTAVE efforts in early April. The third MISRT deferred plans for conducting a risk assessment due to change over in personnel. The DHIAP Team assured that site MISRTs were aware that they were available to assist as needed during their OCTAVE execution, as external technical resources, advisors on executing the methodology, or both. The Team also requested from the site MISRTs and senior MTF management an opportunity to meet periodically with MISRTs to learn of progress and issues in conducting the self-directed risk assessments so that they could gather input for refining the OCTAVE method and training materials to be more supportive of MTF requirements and circumstances.

Results:

Two sites initiated their OCTAVE-based risk assessments in April 2001. Due to the late start date, the active MISRTs were not at a point to share results on lessons learned and issues with the OCTAVE methodology prior to the end of the research period, 31 May 2001.

2.3.7 Provide Method/Training/Templates/Checklists to RIMR (Risk Information and Management Resource)

Methods/Discussion:

As part of the research and development effort for the self-directed risk assessment, the DHIAP Team developed a number of tools for the OCTAVE methodology and integrated them into the documentation and training to support the process. The Team provided the following types of materials to TATRC for inclusion in the RIMR:

- Slide presentations on OCTAVE Methodology that includes presentation outlines for each presentation and instructor notes associated with each slide;
- Method guidelines for conducting an assessment;
- Templates required by the process; and
- Checklists required by the process.

Results:

The DHIAP Team delivered the [OCM] to TATRC prior to start of the MISRT Training Seminars (see Task 2.3.4 Develop/ Deliver SCRA Tutorial) and was used in the initial training for the self-directed risk assessments (see Task 2.3.5 Develop/Deliver SDRA Training).

2.4 Business Case Analysis Task

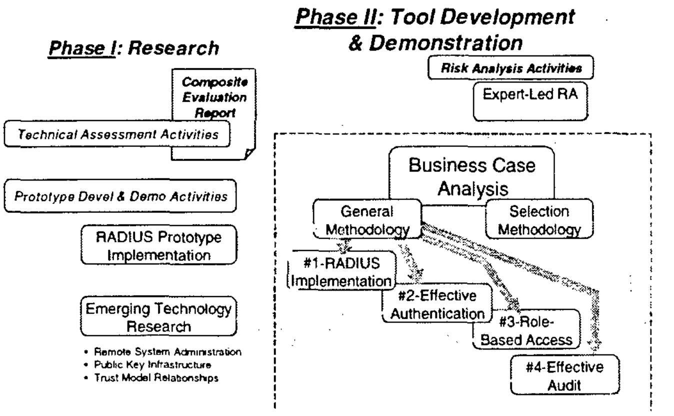

Phase I: Research
Composite Evaluation Report
Technical Assessment Activities
Prototype Devel & Demo Activities
RADIUS Prototype Implementation
Emerging Technology Research
• Remote System Administration
• Public Key Infrastructure
• Trust Model Relationships
Phase II: Tool Development & Demonstration
Risk Analysis Activities
Expert-Led RA
Business Case Analysis
General Methodology
Selection Methodology
#1-RADIUS Implementation
#2-Effective Authentication
#3-Role-Based Access
#4-Effective Audit

Figure 9 – Overview of Business Case Analysis

The statement of work for Business Case Analysis (BCA) calls for analyzing the business conditions affecting the deployment of technologies supporting information assurance in the military healthcare systems and developing a business case methodology to support future analysis of potential information assurance technologies. As appropriate to the purpose of the study, the investigations and the methodology should include an assessment of feasibility, cost, benefit, and availability of information assurance technologies. As depicted in **Figure 9**, DHIAP Phase II BCA activity began with developing a methodology for evaluating the business case for deployment of various information assurance technologies. The methodology was applied in executing BCAs in four diverse situations, and lessons learned from the experience were used to enhance the BCA methodology. To satisfy an immediate project need to determine the subjects that would be investigated with BCAs during Phase II, a self-documenting "selection methodology" was also developed during this effort.

2.4.1 Develop BCA Methodology/ Metrics

The General Methodology was developed as a defined and repeatable process for analyzing the impact on the Department of Defense of deploying technologies for promoting health information assurance in its healthcare system. BCAs are written for Medical Command (MEDCOM) and MTF management faced with implementing a strategy to manage risks associated with vulnerabilities that can be exploited by users and attackers.

Methods/Discussion:

The Team began the Methodology development effort by studying government and industry best practices for conducting BCAs. While this activity provided a useful approach to evaluating such subjects as new computer systems and system upgrades based primarily on increased satisfaction of functional users or cost effectiveness, they did not adequately address circumstances for information assurance which may solve a critical problem but generally does not add to a functional user's effectiveness, increase productivity, or reduce cost.

The Team adapted portions of their basic BCA methodology to incorporate considerations for evaluating important non-cost characteristics of information assurance products, technologies, and implementation approaches (e.g., maintainability, obsolescence, reliability, flexibility, installation requirements, information availability, user acceptance, user training, extent of technical and user setup required, etc.). Additional evaluation categories were defined for risk factors, in particular for project management schedule and financial risks, technical risks, and risks of implementation and/or deployment. The Team tested the initial draft of the General Methodology by conducting the first DHIAP BCA on the processes and technologies that affect the protection of healthcare information in the military.

The DHIAP General Methodology for BCA is the result of iterative refinement. The Team used and refined the methodology as they conducted a series of four BCAs. ("Using" the Methodology for each BCA began with creating a working version specific to the type of BCA and developing the various materials needed to conduct that analysis.) Upon completion of each BCA, the Team updated the General Methodology based on what was learned and/or developed during the conduct of the BCA:

- Upon completion of BCA #1, the Team updated the draft General Methodology based on lessons learned. The updates left the original Methodology basically intact, but altered the sequence of certain initial activities and enhanced the description of how to conduct the various steps.
- An important lesson from writing the final report for BCA #1 was that evaluation results should be reported in terms of "groupings" of individual evaluation criteria in order to reduce redundancy in the BCA report. (In spite of the need to "group" information in order to report it, the Team endorsed the original idea of considering and using a larger number of individual evaluation criteria during the research stage of BCA activity in order to obtain a rich set of data for analysis.)
- The planning process for BCA #2 led to enhancing the General Methodology's lists of evaluation criteria and formalizing the headings under which they were grouped.
- In planning for BCAs #3 and #4 (which were similar in nature), the Team articulated the different styles of analysis for which the Methodology was proving to be effective.

Results:

The *DHIAP General Methodology for Business Case Analysis*, ATI IPT Technical Report 01-04 [GEN], provides an eight-step methodology for analyzing the operational factors, costs, risks, and benefits related to deploying a technology or process. The steps of the Methodology are summarized in **Figure 10**. The first step of the Methodology calls for defining the scope of the BCA. The "scope" is actually a multi-subject summary of what is to be investigated, how, and who is to be involved. A summary of the Scope definition topics is shown in **Figure 11**.

1. Draft initial scope
2. Collect high-level background information
3. Refine scope; define BCA plan and schedule
   - a. Refine scope based on background information
   - b. Develop preliminary report outline
   - c. Identify major work efforts and timeframes
   - d. Develop and refine Evaluation Criteria
   - e. Identify data sources and collection tools
   - f. Refine workplan, assign tasks, schedule external resources
4. Develop data collection tools and methodology
5. Collect and compile data
6. Analyze data
7. Develop key findings, recommendations, and conclusions
8. Write report

Figure 10 – Summary of Methodology Steps

Title	Informative, brief title of analysis
Purpose	Goal or objective of the analysis
Why	Requirement or basis for conducting the analysis
Audience(s)	Consider the level and/or specialized knowledge of the target audience
Timeframe	Elapsed time for completing the analysis (may based on time required, external deadline, etc.); give start and end dates
Cost	Estimated cost of analysis (gives sense of staff size, time allowed, opportunity to travel, acquire technology, etc.)
Type of Analysis	Analysis of Pilot Study, Scenario-Based Assessment, Current/Future Capabilities Assessment, etc.
Functional (User) Target Environment	Type of facility (e.g., regional MTF, community MTF, or clinic) and/or user; deployment setting (e.g., fixed-base CONUS/OCONUS, deployed, shipboard, etc.)
Technical Target Environment/Current Plan	Technical characteristics of deployment setting
General Approach	Methodology or approach for conducting the analysis (e.g., poll of users, literature search, technology development and demonstration, etc.)
Potential Participants	Initially, list types of organizations and individuals expected to participate; over time, expand to become a list of specific organizations/facilities with contact names *Select from military organizations (e.g., regional MTFs, community MTFs, clinics), types of facilities (e.g., fixed-base CONUS/OCONUS, deployed, shipboard, etc.), vendors, facilities using the technologies, publishers of reviews, etc.*

Figure 11 – BCA Scope Definition

2.4.2 Select BCA Subjects and Sites

The subject of BCA #1 had been established in the DHIAP Technical Development Plan. As part of their Phase II effort, the Team worked with TATRC to determine the most important subjects to address in BCAs #2-4. The Team applied their prior experience to developing a selection methodology that was self-documenting so that others could review the basis of the decision and perhaps apply their own reasoning and determine whether or how the final selection might change.

Methods/Discussion:

The Team began developing the process by deciding what factors are critical to a candidate selection process. First, they had to understand the "drivers" that would cause a candidate to be included for consideration or excluded; knowledge of these external influences forms the basis for being able to develop a list of topics to be included in the candidate selection. Next, they had to understand the characteristics against which a candidate should be evaluated; these would be based on such concepts as needs, priorities, barriers, risks, advantages/disadvantages, etc. As a final preparation step, they had to determine the relative importance of each of the evaluation criteria, which they did by assigning each a weighted score. When these parameters were known, the Team was able to begin the evaluation.

Evaluation consisted of building a matrix similar to the table in **Figure 12** (candidate topics across the top, selection criteria/weights down the left side) to use as a decision worksheet. Each team member then scored (using a scale of 0-10 points) the topic against the evaluation criteria; "10" might be assigned if the topic fit the evaluation category exceptionally well, or a low score given if the topic was only minimally relevant to the category. After assigning raw scores to all topics in this way, the team member could look across all of the ratings assigned to determine if mistakes had been made. This crosscheck could indicate the individual's gradual changing of standards through the process, or could allow detection of mistakes. When the scores were determined to be "ready," the Team executed the math to determine weighted scores, see how they had each ranked the topics against each other, determine if something seemed out of line and certain scores should be reconsidered, and then begin to discuss the material as a group.

		Candidate BCA Topics						
		Topic 1		*Topic 2*		...	*Topic N*	
Evaluation Criteria	**Weight** *(0-10)*	Raw Score	Weighted Score	Raw Score	Weighted Score		Raw Score	Weighted Score
Category 1	10	8	80	7	70		5	50
Category 2	8	4	32	4	32		5	40
...								
Category N	3	9	27	6	18		7	21
TOTAL			139		120			111

Figure 12 – Format of Candidate Selection Matrix

The next step was to develop the Team's official ratings for the topics—a process that could be conducted either by merging the individual evaluations or by having the individuals work as a group to develop a "Team" rating. The DHIAP Team chose to execute the latter.

Results:

Topics selected for BCAs #2-4 using the Candidate Selection Process were:

BCA #2: User-Friendly Authentication, which evolved into "Effective Authentication in a Medical Environment" (488 points)

BCA #3: Role-Based Access Control, which evolved into "Role-Based Access Control in an MTF" (515 points)

BCA #4: Network Auditability, which evolved into "Auditing Electronic Access to Military Patient Information" (507 points)

The topics were selected from a group that included computer-based security education, dictation protection, rapid authentication/rapid log-off, and user profiling. Evaluation criteria used in scoring the topics were: customer priorities, available expertise, potential benefit, compliance, impact, appropriateness for Tri-service, risks, breadth of applicability, and existing program in place.

2.4.3 Conduct BCA #1: DHIAP Phase I RADIUS Implementation at Military MTFs

The DHIAP Phase I Prototype Technology Demonstration Task had developed, implemented, and transitioned to operational use a technology capability that was compliant with the Remote

Authentication Dial-In User Service (RADIUS) standard to secure remote dial-in access to information systems. This BCA analyzed the operational factors, costs, risks, and benefits related to installing and using that capability and investigated the costs and operational impact of several approaches to deploying the RADIUS capability across many Medical Treatment Facilities (MTFs).

Methods/Discussion:

The DHIAP Team adapted steps of the [GEN] to be appropriate to the characteristics and goals of the BCA and to serve as the overall plan for completing the research. The Team established the BCA purpose as: Examine the vulnerabilities and requirements that led to the decision to implement a RADIUS-compliant capability at two fixed military MTFs under the DHIAP Phase I in December 1999, consider the costs and risks of these implementations, and compare cost and non-cost factors at each MTF before, during, and after RADIUS implementation.

The Team gathered background material on RADIUS-related technologies and their use from the Internet and other commercial sources and on RADIUS implementation at the demonstration sites from existing DHIAP materials. Based on that information, they planned their approach to performing research and reporting the results and then determined the most appropriate data sources and collection tools for obtaining the methodology's cost factors and non-cost factors data within each category. A unique feature of this BCA is that it examines a subject for which extensive cost/non-cost data was available. Data describing conversion costs was available in accounting records of the DHIAP Phase I participants; operational information and costs of sustaining the pre- and post-implementation environments was available from the Information Management Officers (IMOs), Information Management Division staff (IMD), and operational staff at the two MTFs that had served as Phase I demonstration sites.

To organize the data collection process, the team developed questionnaires to gather non-cost information from staff at the demonstration sites (including users of the remote dial-in service) and a worksheet for collecting cost data. They spent about a half day at each of the demonstration sites, interviewing sites' IMOs and IMD. They arranged for site IMD to deliver the User Questionnaire to users and obtain their responses via the e-mail groups that had already been established for their dial-in users. The Team concluded the data collection activity by merging all interview notes and the results of User Questionniares into data repositories designed to support analysis.

From analyzing the collected information, the team developed a vision of how the technology should be implemented if put into operational use in a larger, more complicated setting such as the Military Health System. They developed recommendations describing two such implementation approaches and used the DHIAP demonstration's cost data to describe the cost outlay and labor effort required for each; as supporting detail for their analysis, they prepared both summary and detailed documentation of the operational and user data collected from the sites. Following in-depth analysis of the operational information that was gathered, they developed the BCA report.

Results:

The *DHIAP RADIUS Implementation Business Case Analysis*, ATI IPT Technical Report 00-08 [RAD], provides an analysis of the operational factors, costs, risks, and benefits related to installing a RADIUS-compliant capability for securing remote dial-in access to information systems. It indicates that key benefits derived from installing RADIUS include:

- Enabling the MTF IMD staff to implement and enforce policies regarding dial-in user authentication and authorization;
- Enabling the MTF IMD staff to explicitly control dial-in user access to MTF systems and resources; and
- Complying with DISC4 policy and improved readiness to comply with emerging HIPAA, JCAHO, and NCQA requirements.

The benefits were achieved with the employed technologies being relatively transparent to operational users and having no real impact on remote dial-in availability, reliability, and communications speed. By assuring that all remote dial-in users passed authentication and were allowed to access requested applications only if proper authorization was in place, the RADIUS implementation allowed sites to improve their security posture and comply with policy and regulatory guidance. The system's relative ease of implementation and use encouraged the MTFs' IMD staffs to extend RADIUS control from the limited test user coverage to all modems on the sites. In addition to evaluating the operational results of the RADIUS implementation, [RAD] describes the costs of implementation (dollars for actual expenditures and in labor hours for work effort) in terms of two operational scenarios, "centralized" and "decentralized." The detailed explanation in the report outlines advantages and disadvantages of each and indicates that a centralized approach is notably less costly than the decentralized approach.

Conclusions of BCA #1:

[RAD] reports that a properly implemented and managed RADIUS-compliant system provides a cost- and operationally-effective means of securing remote dial-in access to information systems. A properly managed RADIUS implementation is an effective and desirable approach to controlling remote user dial-in access. At a relatively low cost, the DHIAP RADIUS implementation satisfied the MTF's need to improve its ability to authenticate authorized users and thereby protect the MTF's information assets from unauthorized user access via dial-in modems. Bringing control of the dial-in access to medical systems from the post's DOIM to the MTF is an important improvement because it places control of dial-in user's authentication, authorization, and audit with the organization that is most knowledgeable about what forms of access should be permitted and which resources are most affected by any negative consequences.

For implementations of this technology beyond the demonstration performed in DHIAP, the [RAD] authors recommend a "centralized" [8] RADIUS implementation as an effective, cost-efficient measure for increasing the protection of sensitive information in the MTF environment. The solution is capable of supporting medical collaboration across a region, and it will also support a regionally based CHCS II enterprise centralization.

[8] In the "centralized" approach, routers are implemented in distributed fashion at all/most MTFs to support local dial-in, while the authorization function is centralized at a primary server at the regional medical center (with a backup device located at one of the community hospitals).

2.4.4 Conduct BCA #2: Effective Authentication in a Medical Environment

Authentication of computer system users in the military Medical Treatment Facility (MTF) environment is critical to the protection of the MTF's information systems and the patient information that resides on many of them. Military policy and regulations require identification of all individuals who access military computer systems and a capability to report their access. Because it establishes the identity of the user, authentication is an essential prerequisite to meeting these access and audit requirements. In addition to the current regulations, information assurance requirements are likely to become more specific as the privacy and security standards of the 1996 Health Insurance Portability and Accountability Act (HIPAA)[9] are formalized.

Methods/Discussion:

The DHIAP Team adapted steps of the [GEN] to be appropriate to the characteristics and goals of the BCA and to serve as the overall plan for completing the research. The purpose of this BCA was agreed as: Analyze capabilities and limitations of various authentication technologies in light of MTF situational dependencies, and present results and indicative costs for acquisition decision-makers.

The Team gathered background material on authentication-related technologies and their use from the Internet and other commercial sources, and also from resources such as the Biometrics Consortium Conference 2000. To gather information about system use and system authorization and authentication practice in today's MTF environment, they used documentation from DHIAP Phase I Information Security Evaluations and participated in certain interviews of the DHIAP Phase II Risk Analysis project. They gathered information about processing of the primary clinical system used by MTFs, the Composite Health Care System (CHCS), and design of the CHCS II system expected to replace it in the near future from Internet resources and interviews with various individuals.

Analysis of the MTF-supplied background information pointed out certain unique operational barriers to making effective use of any authentication technology that might be implemented, including:

- MTFs use many diverse systems, each with its own password-based authentication at point of entry. In such an environment, a traditional implementation of authentication technologies would affect only the user's initial sign-on to the MTF's network, not necessarily sign-on to the applications themselves.
- MTF users may bypass application sign-on controls, and therefore user authentication, by sharing access to terminals. The practice is associated with staff members' need to perform their computer-related work without experiencing the extensive system-imposed time delays that would occur if successive terminal users were to properly log off of a system and then log on to the system and the desired applications.
- Many physical factors in the MTF environment could affect or preclude use of particular authentication technologies (e.g., use of latex gloves affects fingerprint authentication, background noise affects voice detection, etc.).

[9] Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. August 21, 1996. URL: www.aspe.os.dhhs.gov/admnsimp/pl104191.htm.

Based on this knowledge, the Team modified their plans to assure coverage of these subjects, changing from the original purpose and scope of "User Friendly Authentication" to the more pertinent issue of "Effective Authentication in a Medical Environment."

The Team selected evaluation criteria from the [GEN] that were most appropriate for evaluating authentication approaches, also developing additional categories of evaluation criteria that were pertinent to this type of investigation and identified the most appropriate data sources and methods of collecting data within each evaluation category. Recognizing that environmental factors within the diverse operational areas of an MTF should be considered when selecting authentication technologies, the Team defined four representative MTF work environments for evaluating appropriateness of various approaches to user authentication, each offering certain physical and environmental characteristics that affect the use of an authentication technology: Outpatient Clinics, Inpatient Nursing Stations, Clinical Departments, and Administrative Offices.

The Team gathered MTF-related data via interviews with IMD and operational staff at a regional medical center and a community hospital, and also with the design/development team for CHCS II. With the diverse MTF work environments in mind, the Team investigated current and emerging technologies for user-friendly, effective authentication; they used such criteria as security, user acceptance, technical requirements, maintainability, and cost to evaluate passwords, tokens (such as SmartCards), and biometrics (such as fingerprints, voice recognition, iris scans, and facial recognition). Following in-depth analysis of the operational information that was gathered, they developed the BCA report.

Results:

The *Effective Authentication in a Medical Environment Business Case Analysis*, ATI IPT Technical Report 01-01 [ATH], provides the results of the BCA research. As a preamble to aid in understanding its conclusions, the report describes several operational characteristics of MTFs that must be considered and addressed as part of defining the implementation of user authentication technologies:

- It is common in MTFs for staff members to perform their work on a workstation shared among many users. The need to complete tasks rapidly drives the staff to use a session that is already active on the terminal, avoiding the time-consuming process of logging-off a previous user, logging-on correctly, and working through multiple layers of commands to access the desired application. Since staff members using a terminal typically represent a broad range of roles—from physician to nurse, clinical technician, and even the chaplain—and since the roles should have different types of access permissions (for entering vs. only viewing information or not seeing it at all), private patient information could easily be revealed to or modified by unauthorized individuals.
- System users tend to create easily guessable passwords and then use the same password for multiple systems. When issued a "good" password (i.e., one that is hard to guess—but also hard to remember), the users write them down or work to simplify them.
- MTFs do not have consistent procedures for changing passwords or for changing or deactivating user accounts as the user's duty assignment changes or terminates.

The Team's evaluation of current and emerging authentication technologies against such criteria as security, user acceptance, technical requirements, maintainability, and cost produced the following results:

- Passwords are reliable and widely available, although they are also the most highly subject to loss, abuse, and compromise. Since passwords will continue to be an option on computers for the foreseeable future, they should be retained as a valid fallback at least until other authentication modes are fully integrated and have been shown to meet operational requirements. Note that until they are completely replaced by other modes of authentication, organizations will realize little, if any, savings in the cost to support passwords.

- SmartCards are appropriate for most MTF environments and are quite secure when used with a second form of authentication, such as a personal identification number (PIN). Like passwords, they are subject to loss, and the card itself can be damaged. Due to the DOD's SmartCard Program, all military personnel will soon have a DOD SmartCard; the synergy of that program along with local MTF efforts to employ SmartCards for user authentication could significantly reduce program overhead and implementation costs.

- Biometrics are becoming increasingly accurate, cost effective, and easy to use. However, standards for integration, testing, and accuracy reporting are only beginning to emerge and are not consistent. Dealing with a compromised biometric is an extremely difficult task since the personal feature on which it is based cannot be replaced. Depending upon characteristics of particular MTF environments, some biometrics are more useful than others. **Figure 13** summarizes the primary advantages and disadvantages of the four biometric technologies studied.

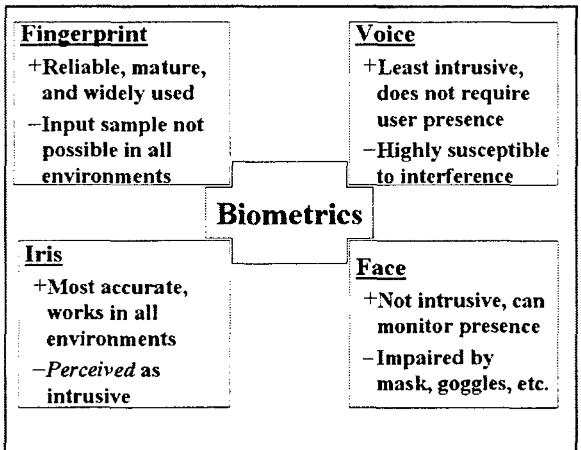

Fingerprint
+Reliable, mature, and widely used
–Input sample not possible in all environments
Voice
+Least intrusive, does not require user presence
–Highly susceptible to interference
Biometrics
Iris
+Most accurate, works in all environments
–*Perceived* as intrusive
Face
+Not intrusive, can monitor presence
–Impaired by mask, goggles, etc.

Figure 13 - Advantages and Disadvantages of Biometric Authentication Modes in an MTF Environment

The fact that MTF systems are presented to users in layers, with the requirement to first sign on to the network and then sign on to individual applications, means that integrating authentication technology at the network level will provide limited, if any, improvement in MTF user authentication. While authentication is necessary for effectively identifying an individual, the work processes of the MTF environment require that certain other supporting technologies also be employed. The following technologies were determined to be useful for making identification and authentication of each system user a practical reality where the terminals are shared by diverse users and staff members' work on the systems must be performed rapidly:

- Automatic Log-Off: In high-traffic, multi-user environments, technology that logs users off a system after a time delay or when the user is no longer in proximity to the terminal would force new users to authenticate, thereby improving the accuracy of audit log data.

- Session Caching: Employment of technology to cache authenticated users' terminal sessions could facilitate an abbreviated (i.e., rapid) re-authentication of returning users.

- Single Sign-On: Where users need access to multiple applications to perform their work, use of single sign-on technology (in which the user authenticates once and, transparent to the user, the system authenticates the user with all other needed applications) would greatly simplify and accelerate the user's authentication process.

Beyond consideration of the technologies described above, the need for user convenience in some MTF environments may necessitate that some workstations offer multi-modal authentication (i.e., provide the user with multiple options for the mode of authentication). Also, certain situations might require the use of multi-factor authentication (i.e., multiple authentication modes such as a SmartCard and PIN used in combination). Implementation of these supporting technologies is a crucial element of making authentication truly effective in the MTF environment.

Conclusions of BCA #2:

While the investigation focused on technology issues, it is clear that technology alone cannot assure effective user authentication. An effective solution requires balanced implementation of sound security policy, good system administration practice, and proper management and use of the technology. Characteristics of the user environment must be considered to ensure that authentication procedure and technology are appropriate to the setting, capable of supporting and not impeding performance of the work.

Although many technologies will appear on Government Service Administration schedules and recommended product lists, the temptation to purchase and implement authentication technology in uncoordinated, piecemeal fashion will significantly magnify the costs, the user frustration, and the impact on the organization's supporting resources. Effective integration of authentication devices and appropriate supporting technologies into the heterogeneous computing environment of the MTF will require extensive planning. The decision-maker must pursue an enterprise-wide, systems-level approach to design. To develop a baseline for effective authentication in an MTF, the authors recommend the implementation of centralized pilot programs that test authentication and supporting technologies in the diverse MTF user environments.

2.4.5 Conduct BCA #3: Role-Based Access Control in an MTF

Controlling user access to computer systems in the military medical treatment facility (MTF) is critical to the protection of the information systems and the patient information that resides on many of those systems. Military regulations specify that access to a sensitive but unclassified information is on "need-to-know" or "least privilege," further requiring that there be a way (e.g., from audit trail data) to identify when and how information was acquired. While a variety of access control methods may be employed, this analysis focused on the current and future capabilities and shortfalls of implementing the widely accepted approach of Role-Based Access Control (RBAC) in the MTF environment.

Methods/Discussion:

The DHIAP Team adapted steps of the [GEN] to be appropriate to the characteristics and goals of the BCA and to serve as the overall plan for completing the research. The purpose of this BCA was: Analyze the current and projected capabilities and limitations of implementing RBAC in an MTF and present results and indicative costs and risks for decision-makers. They defined areas of investigation to include analyzing requirements for role-based access to patient-identifiable medical information and medical/healthcare information systems relative to HIPAA and other regulatory guidance, identifying existing MTF capabilities and planned approaches to satisfying those requirements (considering CHCS and CHCS II and the legacy MTF systems containing patient information not included in CHCS/CHCS II), and assessing technical and operational issues relating to implementation of RBAC.

The Team gathered background material on access control related technologies and their use from the Internet and other commercial sources. For information about system use and access control practices in MTFs today, they initially used documentation from DHIAP Phase I Information Security Evaluations. Then, to identify specific capabilities of MTF systems and determine the extent to which MTFs implement RBAC using these capabilities, they interviewed IMD and user staff of a regional medical center and community hospital about the access control methodologies and technologies of the Composite Health Care System (CHCS) and other representative legacy systems at the MTFs to establish the "as is" level of effectiveness. To obtain information on plans for CHCS II support of RBAC, the Team interviewed members of the CHCS II development team. Evaluation Criteria used in the analysis included: security, technical requirements and maintainability, compliance, user acceptance, and cost. Following in-depth analysis of the operational information that was gathered, the Team developed the BCA report.

Results:

The *Role-Based Access Control in an MTF Business Case Analysis*, ATI IPT Technical Report 01-02 [RBA], reports key findings of the investigation as:

- MTFs have implemented processes for protecting patient identifiable information and for controlling access for individual users.
- MTFs currently implement RBAC at the system/application level in a variety of ways. With CHCS I, the user's role determines which menus he/she sees, thereby controlling the operations he/she can perform. For other legacy systems, RBAC is most commonly implemented informally by a combination of controlling: physical access to the system or application, logical access (via access control lists), file access (by establishing discretionary access controls), distribution and installation of client software, and issuance of application user accounts (requiring separate user authentication).
- MTFs lack a single, MTF-wide methodology for accomplishing RBAC. That is, the methods of implementing RBAC (as described above) and their effectiveness can vary from one system/application to another.
- CHCS II is capable of implementing RBAC because the system was specifically designed (via its Role Matrix and SnareWorks, the backbone of the CHCS II security framework) to implement RBAC. Taking advantage of the CHCS II roles, along with other capabilities built into the security architecture, will reduce the potential for security breaches and should increase compliance with current and emerging laws and regulations. Also, the incorporation of the functionality of the other medical systems in subsequent CHCS II releases should facilitate the MTF's attainment of a formal, MTF-wide RBAC methodology.

Conclusions of BCA #3:

For the MTFs' current systems, the Team found that RBAC capability in CHCS is acceptable, largely due to the formal, well-established manual procedures for implementation of access permissions; role-based access to other legacy systems examined as part of this study is marginal, with RBAC implemented in a variety of informal ways. For MTF processing in the future, CHCS II will offer extensive RBAC capabilities; its Role Matrix provides sufficient granularity and flexibility to serve as a baseline template for MTFs to edit roles according to their needs.

With RBAC, a user's operational capabilities (privileges) are tuned to the organization's working environment to ensure that controls are appropriate to the supporting MTF mission while protecting patient rights and not impeding performance of the work. RBAC is a powerful tool for enhancing information security, reducing the complexity and cost of security administration, but it does not replace good information security practice. Proper user authorization and authentication, along with system audit capabilities are also necessary. Because technology alone cannot assure the effective implementation of RBAC, the solution requires a balance of sound security policy, good system administration practice, and appropriate insertion of technology.

2.4.6 Conduct BCA #4: Auditing Electronic Access to Military Patient Information

Auditing the logs of user activity on computer systems in the MTF is a critical part of a defense strategy to protect the MTFs' information systems and the patient information that is stored on many of them. In support of public law such as the Privacy Act of 1974,[8] military and DOD policies and regulations the capability to report their access (such as could be realized through use of audit trail data). HIPAA will expand the scope of healthcare record keeping requirements.

Specific requirements for healthcare facilities to implement audit capabilities are outlined in the HIPAA Security and Privacy Rules. The proposed HIPAA Security Rule[10] requires audit capabilities that range from reviewing system activity to establishing controls to deter, detect, and assess security breaches; the HIPAA Privacy Rule[11] stresses the protection of a patient's privacy and allows a patient to request a historical record of disclosures (i.e., an audit trail). Even though the HIPAA requirements primarily dictate exercise of good security practice, the effort of implementing the capabilities they require may significantly impact current MTF operations.

Methods/Discussion:

The DHIAP Team adapted steps of the [GEN] to be appropriate to the characteristics and goals of the BCA and to serve as the overall plan for completing the research. The purpose of this BCA was agreed as: Analyze the current and projected capabilities and limitations of audit capabilities in an MTF, and present results and indicative costs and risks for decision-makers. Areas of investigation were defined to include analyzing the information and information systems audit requirements, identifying existing capabilities and planned approaches to satisfy those requirements, and analyzing impact and shortfalls of those approaches.

The Team gathered background material on the capabilities of audit related technologies and their use. For information about system use and system audit capabilities practiced in MTFs

[10] See *Security and Electronic Signature Standards*; Proposed Rule. Office of the Secretary, U.S. Department of Health and Human Services. Part III, 45 CFR, Part 142. Federal Register, Volume 63, Number 155. 12 August 1998. URL: http://aspe.hhs.gov/admnsimp/Index.htm.

[11] See *Standards for Privacy of Individually Identifiable Health Information*; Final Rule. Office of the Secretary, U.S. Department of Health and Human Services. Part II, 45 CFR, Parts 160 and 164. Federal Register, Volume 65, Number 250. 28 December 2000. URL: http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy

today, they studied documentation from DHIAP Phase I Information Security Evaluations. To identify audit capabilities of current MTF systems and to determine the extent to which MTFs utilize these capabilities, they interviewed IMD staff of a regional medical center and community hospital to examine audit capabilities of the MTFs' primary health care system, Composite Health Care System (CHCS) and representative legacy systems at the MTFs. Through interviews with the CHCS II development team, they examined the plans for audit capability in this system that will soon replace CHCS. Evaluation criteria used in analyzing audit effectiveness included: security, technical requirements and maintainability, compliance, user acceptance, and cost. Following an in-depth analysis of the operational information that was gathered, they developed the BCA report.

Results:

The *Auditing Electronic Access to Military Patient Information Business Case Analysis,* ATI IPT Technical Report 01-03 [ADT], reports that CHCS offers adequate audit capability, and MTFs have well-established procedures for auditing users on this system. Other legacy MTF systems examined as part of this study are marginally capable of implementing audit controls, and some lack audit controls altogether. CHCS II will offer MTFs a more comprehensive security framework. Other key findings include the following:

- All MTF systems processing sensitive but unclassified information (i.e., protected patient information) must be Class C2 certified. However, the *DOD Trusted Computer System Evaluation Criteria*[12] (colloquially known as "The Orange Book") that specifies the certification requirements was published in 1985, making it often ineffective for application to some newer technologies and technical requirements in use at the MTFs.
- Class C2 certification may present a false sense of compliance since many of these trusted systems will not meet HIPAA audit requirements.
- Some systems (e.g., CHCS) are capable of recording detailed log data sufficient to create an effective audit trail, but the extent of utilization of these capabilities varies with the site.

Conclusions of BCA #4:

Audit logs serve as an effective means of deterring authorized users from abusing privileges and is also somewhat effective in deterring attacks.[13] In addition, audit logs are useful in investigations to identify and assess damage resulting from attacks and, subsequently, to serve as evidence of the attack. The overall usefulness of audit logs, however, depends upon whether they are kept, the detail to which the events are captured, and whether they are reviewed.

CHCS offers MTFs adequate logging capability, as will its CHCS II replacement. For the other legacy systems in use at MTFs the situation is different. There is no simple, economical way to audit access to patient information when, as is true for many MTF legacy systems, the capability was not designed into the application and/or patient records do not correlate directly to files. With the exception of CHCS, MTFs' current audit log capabilities are limited by the systems

[12] *Department of Defense Trusted Computer System Evaluation Criteria*. DOD 5200.28-STD. December 1985.

[13] Clayton, Paul D., et al. *For the Record Protecting Electronic Health Information*. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. National Academy Press, Washington, D.C. 1997

themselves, and the absence of log capability in many systems puts MTF information assurance at risk.

Even when audit capability is available in a system, the system administrators often have freedom to select the types and extent of auditing that is done. This fact emphasizes the importance of assuring that operational procedures require the type of auditing that permits the MTF to be in compliance with all applicable regulations and to have the type of audit trails that allow them to use log data effectively for documentation and research. To meet the audit requirements, MTFs need two general types of audit logs: Security Logs (capturing events ranging from authentication success/failure to application execution and object access) and Privacy Logs (capturing disclosures of patient identifiable information in accordance with Section 164.528 of HIPAA Privacy Rule[11]). In addition, they will need a third supporting log, the Unauthorized Access Log (capturing access control violations), to supplement the privacy logs when required.

2.5 Simulation Capability Task

Experience of recent years has indicated a need for fundamentally new approaches to security and survivability of large-scale networked systems. Infrastructures and other modern systems pose problems of dealing with partial information, complexity of combinatorial interactions of very large numbers of human and automated participants, ubiquitous access, loss of centralized administrative control, the growing threat of automated attacks and recognition that availability of services is becoming essential to mission accomplishment. Survivability research seeks new methods including emergent algorithms, diversity and dynamic trust validation to ensure that systems satisfy their most critical requirements. Easel is an automated simulation tool for research in survivability, infrastructure assurance and other applications that must contend with incomplete and imprecise information. As depicted in **Figure 14**, the usefulness of such a capability in assessing the state of information assurance in the military healthcare system was identified during Phase I research activities. The purpose of the Easel project is to design a modeling and simulation language suitable for doing research in survivability of unbounded networks, and to produce a prototype implementation of that language.

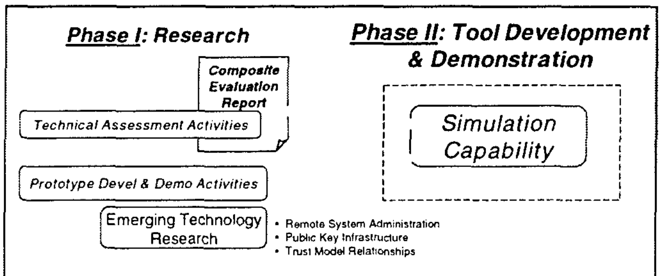

Phase I: Research
Phase II: Tool Development & Demonstration
Composite Evaluation Report
Technical Assessment Activities
Prototype Devel & Demo Activities
Emerging Technology Research
• Remote System Administration
• Public Key Infrastructure
• Trust Model Relationships
Simulation Capability

Figure 14 – Overview of Simulation Capability

2.5.1 *Develop/Demonstrate Survivability Simulator*

Methods/Discussion:

The first step in the Easel project was to examine the requirements of simulation of emergent algorithms in unbounded systems and determine whether those requirements could be met using existing programming languages. The conclusion was that they could not. Having established that no traditional simulation language met the requirements of simulating emergent algorithms in unbounded systems, a new approach to simulation was adopted called Easel, an emergent algorithm simulation language and environment. Easel is designed to employ a paradigm of property-based types (i.e. describing abstract classes of examples by their shared properties) to simultaneously address the above listed simulation issues.

As part of the project, The DHIAP Team compared Easel to a wide range of existing programming languages; the results are summarized in **Figure 15**. For purposes of the comparison existing languages were placed in five categories, as follows: (1) General purpose discrete event simulation languages such as Simscript, Simula, and GPSS (labeled G in the Figure); (2) Special purpose simulation languages like Extend, Arena, or iThink (L); (3) Ad hoc discrete simulation packages such as Swarm and MAML (D); (4) Dynamic or continuous simulation systems (C); and (5) StarLogo - a language designed to study the distributed mindset and unbounded thinking (S). As **Figure 15** shows, Easel has many features that make it ideally suited to its application domain relative to other languages.

The DHIAP Team executed the Easel project using a modified spiral development lifecycle model. Using the requirements document as a guide, they developed a language specification in the form of a Language Reference Manual (LRM); that document served as the basis for the Easel Author's Guide (a document to assist Easel programmers in learning the language), the implementation, and the Easel Validation Suite (a suite of self-checking tests to measure conformance to the language specification).

	C	L	D	C	S	E	
Modeling							
abstract models •						Y	
accurate /incomplete specification •						Y	distributed
specification					Y		
reusable						Y	
Simulation							
autonomous actors •		S	PS		P	Y	
scalable to large numbers of actors •		S	S	S	P	Y	
general purpose	Y		Y	S		Y	
representation independent		P				Y	
database interface	S	Y	Y	Y		Y	
dynamic simulation capability				Y		Y	
statistical package	S	S	Y	Y		Y	
Neighbor Relationships							
built-in support		Y				Y	
dynamic topology •	Y		Y		P	Y	
arbitrary dimensional •	Y		Y	Y		Y	
declarative						Y	
Graphic Depictions							
built-in support	S	Y	S	Y	Y	Y	
multiple views		S	S	S		Y	
dynamic graphic	S	S	S	S	Y	Y	
general purpose	S		S			Y	
scalable graphics			?			Y	
declarative						Y	
distributed specification						Y	
automatic composition						Y	
essential	2	2	4	2	3	6	/6
optional	6	9	11	8	5	22	/22

Figure 15 – Comparison of Modeling and Simulation Systems

Results:

Because Easel is property-based it can be used to give accurate, but incomplete, descriptions of anything. In combination with an appropriate automated logic system, it can be used to produce accurate conclusions about examples from the physical world. This contrasts with physical models and automated simulations that depend on representation of objects, where descriptions must be complete (and thus inaccurate) and in which conclusions are accurate only for the model but never for their extensional interpretation in the real world. While traditional modeling and simulations systems answer all questions without a mechanism for user to determine which answers are accurate, Easel reports what additional information is needed to continue toward an accurate result. Easel also supports multiple levels of abstraction, multiple simultaneous belief systems, distributed specification and dynamic graphic depictions.

Easel is a discrete event simulation language plus limited support for continuous variable. The linguistic limitations of traditional programming systems for incomplete and imprecise description are overcome by use of quantifiers, adjectives, improper nouns, pronouns and other forms of anonymous reference in the language. In combination with property-based types, these mechanisms provide a semantic framework of examples of any type whether real or imagined and whether from the computational, mathematical or physical worlds.

Figure 16 depicts the architecture of the entire simulator system. Starting with the author, and moving counterclockwise through the system, the major components of the system are as follows:

- The *graphics editor* allows direct user manipulation of graphics objects and saves the results as Easel code that can then be imported into programs.
- The *text editor* has not yet been implemented, because the availability of many native text editors on the host makes it a low priority.
- The *lexical analyzer* and the *parser* produce parse trees that are optimized for interpretation. The parser utilizes a shift-reduce scheme combined with precedence parsing for expressions. The parser uses an *include mechanism* that supports the construction and use of Easel libraries. It also includes a *dimensional analysis subsystem* that checks Easel programs for errors in dimensions and units, and a general-purpose *error reporting facility* that works by decorating the parse tree with arbitrary annotations that are then handled by the pretty-printer.

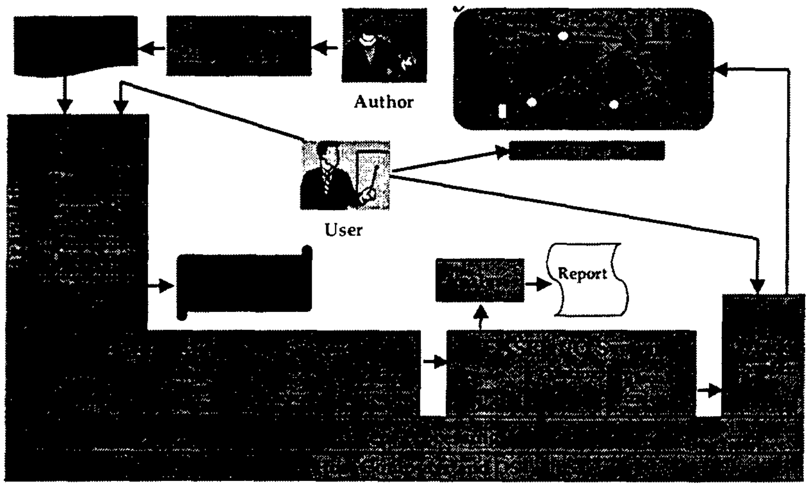


Figure 16 – Components of the Easel Simulation System

- The *code generator* decorates the parse tree with the offsets of variables relative to the stack frame; this is an optimization that improves run-time performance.
- The *semantic analyzer* performs run-time overload resolution and type matching. Easel is unusual in that it supports very late typing, which means that not all overload resolution must be done at compile time.
- The *memory manager* features a high-performance data representation that is optimized for Easel data structures. It includes an innovative garbage collection algorithm to relieve Easel programmers of the need to explicitly de-allocate memory.
- The *scheduler* manages multiple threads of control in actors at run time. Its design has been carefully engineered to be a good match for Easel's intended application domain, and frees the programmer from most of the complexity of traditional thread management.
- The *interpreter* executes off the tree representation produced by the parser as transformed by the code generator and semantic analyzer. Threaded-code interpreters inspired its design, in that most of the operations are factored out into operators accessed through jump tables. These include operators for numeric operations, operations on data types

(arrays, lists, enumeration types), graphics primitives, actors, and property-based type operations. In addition the system provides a large library of statistical and other math functions useful for simulations.

- The *analysis subsystem* is currently illustrated by the Easel Validation Suite, which generates XML output that is then manipulated using standard XML tools.
- The *I/O subsystem* is currently limited to textual input and output. The Easel prettyprinter can produce textual representations of any Easel program or data structure.
- The *dynamic graphic depiction subsystem* displays depictions for actors at run time, relieving authors of many of the details of representing their simulations.

The alpha release of the system has been used on a number of student projects at Carnegie Mellon University. Although no formal user testing has been performed, initial feedback has been positive.

2.5.2 Provide Preliminary Manual and Guide

Methods/Discussion:

Using the requirements document as a guide, a language specification was developed in the form of a Language Reference Manual (LRM). The LRM document and the lessons learned in language development and testing served as the basis for the Easel Author's Guide (a document to assist Easel programmers and users in learning the language).

Results:

The *Easel Language Reference Manual, Version 1.0* [LRM] was published as a draft in July 2000 and published as version 1.0.3.3 in October 2000. The *Easel Author's Guide: An Introduction of the Easel Simulation Language and its Environment* [EAG] was published in draft form in February 2001. Both reference documents are maturing as the simulation capability matures.

2.5.3 Coordinate with Advisory Groups and Conduct Technical Meetings

Methods/Discussion:

Coordination with simulation advisory groups was envisioned as a means to get expert review of the utility of the simulator and to ensure that the capabilities being developed meet the potential users needs. Since the advisory groups proposed were to consist of experts in the areas of simulation and healthcare, the government program manager took the responsibility to recruit the members and to plan for and schedule the meetings. Due the challenge of identifying the appropriate participants and difficulty of scheduling a common time and place to meet, the proposed technical meeting of a Simulation Advisory Group never occurred. Alternative proposed was a technical briefing to the already established Medical Health Systems' Information Assurance Working Group. That technical briefing was never scheduled.

Results:

No advisory group focused on simulation was formed and no technical meetings outside the scheduled program reviews and demonstrations to the government program managers were held.

THIS PAGE INTENTIONALLY LEFT BLANK

3. Conclusions

The DHIAP Phase I and II efforts succeeded in researching the state of information assurance for military healthcare information and in developing and demonstrating in field trials new tools and techniques to allow individual organizations from MTFs to centralized authorities evaluate and manage their own facilities' state of information assurance. While the tools were developed for use in information assurance in the healthcare environment, they are adaptable and equally applicable to other areas of focus and even to other operational settings.

This report describes the work completed in the Phase I research and Phase II tool development, testing, and analysis program activities (see **Figure 17**). In Technical Assessment, the DHIAP Team conducted ISEs at two MTFs and used results to develop recommendations for improving information assurance capability for MTFs in general and for military healthcare system overall. In Prototype Development/Demonstration/Transition, the Team developed, tested, and transitioned to MTF operational use a capability for assuring the identity and controlling system access of remote dial-in users of computer systems. In Risk Analysis, the Team developed and tested a methodology and tools for assessing risk to information assets. In Business Case Analysis (BCA), the Team developed a methodology for analyzing operational impact to the military of deployment of technologies affecting healthcare information security, and exercised and refined the Methodology during the course of conducting BCAs in four investigations of information assurance technologies. Technologies investigated were remote authentication of dial in users, authentication, role based access control, and audit of computer use and access. In Simulation Capability, an alpha version of a survivability simulator designed to assess impact on mission survivability was created and functional capabilities were demonstrated.

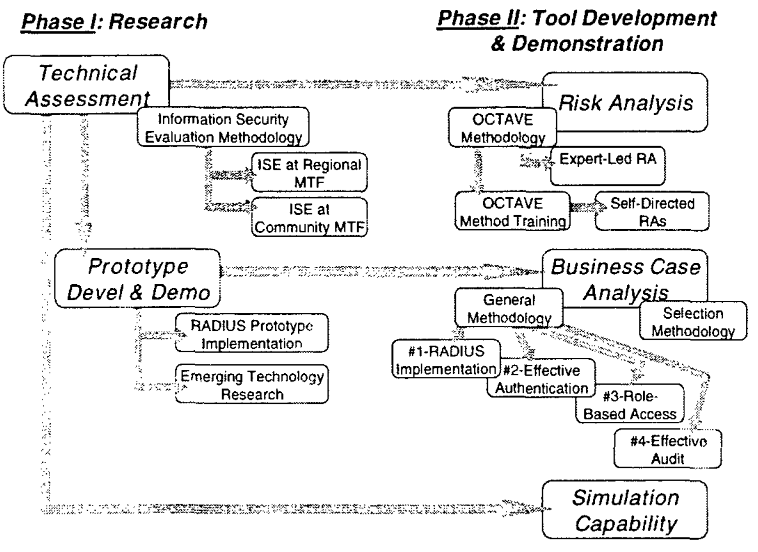


Figure 17 – Information Flow from Research to Operational Use

3.1 Technical Assessment Task

Task Overview: This task focused on evaluating medical information systems. The ISEs served to establish an organization's baseline information assurance capabilities and vulnerabilities, and from the ISEs, the Team recommended operational policies and procedures to address those vulnerabilities.

Summary of the Effort: Working in conjunction with the sites' IMD staffs, the Team found a significant number of minor to critical vulnerabilities to the MTF information systems that were both specific to the MTF and systemic to the entire MHS. The Team worked with the different operational levels of the MTFs, providing the IMD staffs with guidance on fixing the vulnerabilities, and the MTF leadership and higher headquarters with awareness of the security issues facing their facilities. For their part, the MTF staffs took actions within their authority and capability to improve their security posture and forwarded those issues beyond their control up their operational chain of command for resolution. The ISE method and results were also briefed to the MEDCOM CIOs.

Conclusions: MTFs' information systems are vulnerable to abuse, attack, and compromise. As a result of the ISEs, MTF staffs at the evaluated sites have taken numerous steps to improve their security posture (e.g., developing and enforcing procedures to deter password sharing among users); however, the staffs often lack the training, funding, time, and authority to fix all vulnerabilities. Enterprise-wide solutions are needed to leverage lessons learned from individual MTFs and to fully address all issues, particularly to deal with those issues that are beyond the capability of local MTFs. MTFs needed a self-supporting tool to conduct risk analyses in order to prioritize information assurance risks and develop mitigation strategies.

3.2 Prototype Development, Demonstration, and Transition Tasks

3.2.1 RADIUS Implementation

Task Overview: The purpose of this task was to implement and validate proposed security solutions stemming from the Technical Assessment Task's ISEs.

Summary of the Effort: The DHIAP Team studied the technical vulnerabilities identified in the ISEs for areas where application of technology could reduce or even resolve significant exposures. A review of alternatives with representatives of the MTFs that would serve as trial sites for the technology demonstration resulted in the decision to build a prototype that would provide Army-mandated compliance with the Remote Authentication Dial-In User Service (RADIUS) standard. The Team worked closely with MTF technical representatives to confirm Army requirements relative to RADIUS, and then examined the marketplace for hardware and software components that met the requirements and satisfied many of the technical preferences expressed by MTFs participating in the effort. After building and testing a prototype in a laboratory environment, the Team implemented it at the MTFs, developed installation and operating procedures to guide initial users of the system, and transitioned the technology to the sites for permanent use supporting remote dial-in users.

Conclusions: The RADIUS demonstrations improved both security and availability for dial-in users. The sites were able to authenticate dial-in users, control their access, and log (for audit records) their actions. Sites established procedures to remove other, unauthorized modems, and users were migrated to RADIUS.

The RADIUS demonstration clearly showed the ease of implementing the RADIUS-compliant system in the military's existing regional network environment, its ability to work within the regions' and sites' Windows NT-based technical environment, and its effectiveness in controlling and auditing remote dial-in users of military healthcare systems. The demonstration sites have successfully transitioned the prototype to full operational use.

Successful pilots, such as the RADIUS demonstration, not only consider the operational environment and its needs, but also involve the user(s) in the formation/design of the solution. Additionally, before the solution is introduced to the operational environment at the demonstration sites, the technical prototype should be validated in a lab environment. Such user involvement and operational testing is critical to user acceptance. Continued support (maintenance, staff, funding, etc.) is also necessary for long-term system sustainment.

3.2.2 Emerging Technologies

Task Overview: Based on the ISE findings, knowledge of emerging technology, and MTF policies, the DHIAP Team studied key areas of research pertinent to the security issues facing the MTFs immediately or in the near future. The areas of investigation and research included: Public Key Infrastructure, trust models (i.e., defining and applying trust relationships in a networked computing environment), and remote system administration.

Summary of the Effort: The DHIAP Team worked closely with MTF technical representatives and TATRC to confirm Army requirements relative to three research topics and then examined the technology issues in terms of the operational environment. Key findings can be summarized as follows:

- The Public Key Infrastructure (PKI) paper provides analysis of the potential impact on the medical health systems of implementing PKI, perspective on other programs which have implemented PKI, and an explanation of how PKI encryption works and how the keys are handled.

- The trust model paper provides an analysis of intentional and unintentional trust that is granted to users, systems, and networks, utilizing concrete examples (the web server and remote system administration) based on situations discovered in the ISEs.

- The remote system administration paper describes an issue that was found to be prevalent during the ISEs. While "stove pipe" systems are part of an MTF's normal support mechanisms, this paper examined the risk that external system access and administration incurs, and provided suggestions for handling security gaps in this environment.

Conclusions: The Emerging Technology whitepapers outline particular information assurance issues faced within DoD, and in particular, within Army MTF information architectures. Involvement of the MTF sites, to fully understand their operational environment, was key to the usefulness of this research effort. The papers serve as a preliminary analysis/research of technology prior to more exhaustive business case analysis and/or pilot testing.

3.3 Risk Analysis Task

Task Overview: Based on the conclusions cited in the Technical Assessment Task, this task developed the methodology to identify and rank risks to healthcare information assurance and define mediating/mitigating actions and strategies.

Summary of the Effort: The OCTAVE method is a tool that can be used to identify an organization's critical assets; identify the threats, vulnerabilities, and subsequent risks to those critical assets; and develop action plans and mitigation strategies to address the risks. The methodology depends upon the participation of site personnel since they understand the importance of their assets. Applicable across service boundaries, Army, Air Force, and Navy sites have participated and/or been trained in OCTAVE, making it ready for widespread dissemination to all military healthcare facilities.

Conclusions: Because it is infeasible for outside experts (whether government or contractor) to visit each MTF and conduct information security assessments, the Risk Analysis task provided the military with a tool for sites to conduct their own security assessments. Furthermore, the OCTAVE process, because it requires site personnel participation, provides a product that is developed and owned by the site, not just a report provided by outsiders. While the Risk Analysis task provided the tool for individual sites, the military still needs a feedback mechanism to identify and address enterprise-wide issues and prevent sites from developing stovepipe solutions.

The limited and delayed participation in OCTAVE training and then sites initiation and completion of their risk assessment investigations indicated to the DHIAP Team that it is critical to have active support from the MACOM. MTF commanders face a constant challenge to meet all mission requirements. The interest of a site's command group in performing a risk analysis seemed completely dependent on whether the MACOM considered the effort to be important. Without the MACOM establishing completion of the OCTAVE as a priority task, it could get lost among the mission critical tasks. This observation is supported by DHIAP's need to have the Surgeons General direct sites to participate in MISRT training. Once the risk analysis effort is made a priority for the site, it becomes necessary for the site's higher echelons to be actively involved as overseers of the work. It is only with this oversight and attention that adequate resources are made available, that the resources are available at each step of the process, and that the sites are empowered to execute the process in a site-defined "reasonable" timeframe.

3.4 Business Case Analysis Task

Task Overview: Stemming from the Prototype Demonstration, Development, and Transition Task, and from the Emerging Technologies Task, this task involved the development of a General Methodology to assess the basis for deployment of information assurance technology. As an extension of the General Methodology development, four BCAs were conducted on information assurance technologies.

Summary of the Effort: Lessons learned from each BCA contributed to and enhanced the development of the General Methodology. The General Methodology evolved into a flexible, adaptable, eight-step process for developing a business case based on a set of evaluation criteria that can be tailored for the specified information assurance technology or process to determine tangible (e.g., cost) and intangible (e.g., operational and security) benefits. The end result was a defined, repeatable process useful to MTFs and other organizations for analyzing their information assurance needs and prioritizing requirements. The four BCAs to which the evolving General Methodology was applied were: the DHIAP RADIUS implementation, user authentication in a medical environment, role-based access control, and auditing electronic access to patient data.

Conclusions: Military program managers need a tool that examines the operational, functional, and technological impacts, as well as the costs and risks, of deploying a new technology. The General Methodology proved to be flexible and adaptable for diverse investigations, while recognizing the military perspective in describing a business case. The General Methodology provides a tool that can be used at any level, from MTFs to MEDCOM, OSD/HA, and other agencies, where acquisition decision-makers need to develop or implement new or improved technologies or processing capabilities. Although it was developed for investigating healthcare information assurance technologies, it is equally applicable to other emerging technology areas and other military and non-military environments.

The BCAs conducted in DHIAP provide in-depth topical analyses, enabling decision-makers to narrow choices from a broad range of available technologies down to those most appropriate for an organization's information assurance requirements. Such BCAs are a valuable tool to assess the value of a technology or process (before investing heavily in deployment/fielding).

3.5 Simulation Capability Task

Task Overview: Stemming from the Technical Assessment Task and the Prototype Demonstration, Development, and Transition Task, this task developed tools and methodology to simulate mission survivability of the DoD healthcare infrastructure.

Summary of the Effort: The DHIAP Team developed the Easel simulation language for modeling open, unbounded problems. Executing a modified spiral development model, the Team started by designing the system architecture and building the fundamental components of a simulation language and a simulator system. The fundamental capabilities of the simulator have been demonstrated. The next step is to develop and demonstrate models pertinent to military medical information infrastructure.

Conclusions: The study of threats, vulnerabilities, and risks associated with operational requirements of diverse information assets and heterogeneous logical networks are open, unbounded problems. The military needs tools to analyze such problems before risking time and money in deploying new technologies. Asset and network properties can be captured in models to form re-usable components for simulations that theoretically identify information security gaps and analyze the operational impact of information assurance protection strategies. Easel is an automated simulation tool for analyzing potential effects of predictable and unforeseen events on modern, unbounded systems that can only be described with incomplete information.

THIS PAGE INTENTIONALLY LEFT BLANK

4. References

[CER] Andrews, Archie D., et al. *DHIAP Phase I Composite Evaluation Report.* Advanced Technology Institute. ATI IPS Technical Report 00-02. DAMD17-99-C-9001. February 2000. URL: http://ips.aticorp.org/TR/.

[IMG] Melton, Lane, *DHIAP Supplemental Installation and Maintenance Guide.* ATI IPT Special Report 00-03. DAMD17-99-C-9001. April 2000. URL: http://ips.aticorp.org/TR/.

[TDR] Crane, Lynn, et al., *DHIAP Phase I Technology Demonstration Report: Prototype for Remote Authentication Dial-In User Service (RADIUS).* ATI IPT Technical Report 00-04. DAMD17-99-C-9001. April 2000. URL: http://ips.aticorp.org/TR/.

[RSA] Packard, Stephen L. and Archie D. Andrews. *Remote System Administration: Issues and Recommendations.* ATI Special Report IPS 00-01. DAMD17-99-C-9001. April 2000. URL: http://ips.aticorp.org/TR/.

[PKI] Streetman, Kibbee D., et al. *Public Key Infrastructure: Resources, Requirements, and Recommendations.* ATI IPT Special Report 00-06. DAMD17-99-C-9001. April 2000. URL: http://ips.aticorp.org/TR/.

[TRU] Stinson, Jack, et al., *Trust Model: Defining and Applying Generic Trust Relationships in a Networked Computing Environment.* ATI IPT Special Report 00-07. DAMD17-99-C-9001. May 2000. URL: http://ips.aticorp.org/TR/.

[SIM] Fisher, David, *Survivability and Simulation*, personal correspondence of the author, August 2000.

[OCM] Alberts, Christopher J. and Dorofee, Audrey J., *OCTAVE Method Version 1.0 Implementation Guide*. January 2001. URL: http://www.tatrc.org (from home page, select RIMR, Assessments).

[OFL] Alberts, Christopher J. et al., *OCTAVE*^{SM} *Final Report, DOD Medical Treatment Facility*. DAMD 17-99-C-9001. December 2000.

[GEN] Pellissier, Stephen V., et al. *General Methodology for Business Case Analysis.* Advanced Technology Institute. ATI IPT Technical Report 01-04. DAMD17-99-C-9001. May 2001. URL: http://ips.aticorp.org/TR/.

[RAD] Crane, Lynn S., et al. *DHIAP RADIUS Implementation Business Case Analysis.* Advanced Technology Institute. ATI IPT Technical Report 00-08. DAMD17-99-C-9001. October 2000. URL: http://ips.aticorp.org/TR/.

[ATH] Pellissier, Stephen V., et al. *Effective Authentication in a Medical Environment Business Case Analysis.* Advanced Technology Institute. ATI IPT Technical

Report 01-01. DAMD17-99-C-9001. January 2001. URL: http://ips.aticorp.org/TR/.

[RBA] Pellissier, Stephen V., et al. *Role-Based Access Control in an MTF Business Case Analysis.* Advanced Technology Institute. ATI IPT Technical Report 01-02. DAMD17-99-C-9001. April 2001. URL: http://ips.aticorp.org/TR/.

[ADT] Pellissier, Stephen V. et al. *Auditing Electronic Access to Military Patient Information Business Case Analysis.* Advanced Technology Institute. ATI IPT Technical Report 01-03. DAMD17-99-C-9001. May 2001. URL: http://ips.aticorp.org/TR/.

[LRM] Fisher, David et al. *Easel Language Reference Manual, Version 1.0, Draft Review Copy.* July 2000.

[EAG] Fisher, David et al. *EASEL Author's Guide: An Introduction of the Easel Simulation Language and its Environment, Draft.* CMU/SEI-2000-TR-33. February 2001.

[TD1] Andrews, Archie D., et al. *Defense Healthcare Information Assurance Program Technical Development Plan.* Advanced Technology Institute. DAMD17-99-C-9001. November 1998.

[TD2] Andrews, Archie D., et al. *Defense Healthcare Information Assurance Program Technical Development Plan DHIAP Phase II, Version 4.0.* Advanced Technology Institute. DAMD17-99-C-9001. December 2000.

5. Appendices

Appendix 1 – **Defense Healthcare Information Assurance Program Technical Development Plan (Phase I)**

Appendix 2 – **Defense Healthcare Information Assurance Program Technical Development Plan DHIAP Phase II, Version 4**

THIS PAGE INTENTIONALLY LEFT BLANK

Defense Healthcare Information Assurance Program
Technical Development Plan

General

The purpose of this document is to describe the technical plan and schedule in sufficient detail to follow progress and guide execution to ensure that government objectives are met within budget.

This is a living document that will change as the execution of the program proceeds. It should be viewed as a draft that is under revision as the program is executed and unknowns are resolved.

The format of this plan is background information followed by a detailed description of the areas of work and the tasks that make up those major areas. Each task will have a brief paragraph of explanation followed by key events and, since this is an event driven program rather than a calendar driven program, a listing of critical dependencies. An estimated schedule expressed in work days is included for each task. This schedule estimate is expressed in work days rather than calendar days, thus, a task that is estimated for 30 work days will take 6 calendar weeks as a minimum. Following the detailed description of the program is the Work Breakdown Structure to illustrate sequencing, dependencies and a schedule of events for progress tracking.

Background

The objective of the Defense Healthcare Information Assurance Program (DHIAP) is to ensure that clinical and other health related data of DoD active duty personnel and other beneficiary populations are readily accessible but only to authorized healthcare providers. The method proposed to reach this objective is development and demonstration of a series of protected information systems supporting the Military Health Systems. The DHIAP will:

- Evaluate existing medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities,
- Validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems,
- Provide technical and programmatic advice regarding long range programs to address information assurance vulnerabilities,
- Provide authorized users appropriate, secure access to data resources from typically non-secure environments such as the Internet,
- Implement the systems effectively and efficiently for evaluation within the military-civilian medical community.

Lessons learned from the project will provide the Army and the Military Health Systems with a greater understanding of the threat to protection of healthcare information and the measures available for deployment within the existing healthcare information system infrastructure. The demonstration prototypes will assist in defining a long-term program that provides the flexibility to respond to a changing threat, maintain information assurance continuity with the civilian healthcare component, and respond to military requirements for information and operational security.

Program Description

DHIAP consists of four major areas of work: Technical Assessments, Prototype Development, Demonstration, and Technology Transfer. Work areas are expanded in the following work breakdown structure and schedule of events.

TECHNICAL ASSESSMENTS

The government-contractor team will perform on-site technical assessments of the selected Alpha testbed sites to reveal system security issues and site security requirements. This work is subdivided into four composite tasks: site selection, preparation for site evaluation, the actual evaluation of each site, and creation of a composite report on the evaluations.

Site Selection

TATRC has agreed to nominate a set of potential sites for review by the evaluation team. Pre-nomination coordination with the site will be accomplished so the request for information reaches a ready and receptive audience. The sites will provide initial baseline information on their security systems and organizational support. The evaluation team will recommend testbed sites based on an initial analysis of this site-provided information.

Key Events:

- Sites will be nominated for inclusion in the alpha phase by TATRC.
- Contractor will supply baseline survey instrument.
- Baseline information describing the existing information security posture will be requested from the sites by TATRC.
- The government-contractor team will review supplied information and recommend sites to include in technical assessment as well as justification for the recommendations.
- Sites will be notified of results of initial screening and decisions based on recommendations.

Dependencies: Sites agreement to participate.

Schedule: Task estimated to require 32 work days from start to decision on test bed sites. That includes requisite time for the sites to agree to participate and to prepare their response to the initial request for information.

Site Evaluation Preparation

The evaluation team will be lead by the Software Engineering Institute CERT member and composed of members from the Software Engineering Institute, Lockheed Martin Energy Systems, the Advanced Technology Institute and the Government. The methodology executed will be the SEI's Information Security Evaluation.

Key Events:

- Determine roles required for site evaluation team.
- Resolve who will participate in site evaluation and availability of personnel.
- Site evaluation training at Software Engineering Institute in Pittsburgh, PA.

Dependencies: Availability of participants and SEI training team.

Schedule: Task estimated to require 30 work days. This task can occur concurrently with the site selection task but the training event should occur after test bed site decision.

Site Evaluations

Site evaluations will be conducted on up to three sites. The evaluation will follow the SEI developed Information Security Evaluation format and methodology. In order to foster an open, problem and solution identification cooperative process, the findings and recommendations associated with any single site will be disclosed to that site only unless explicit permission is given to share the results. Conclusions based on generic findings will be provided to others but disassociated from specific sites. The methodology consists of a six step process: site briefing to the command group and the involved parties (Information Systems administrator, Security staff, and users); data collection by site personnel; team preparation; onsite data collection; data analysis; and feedback on the evaluation.

The initial site briefing will explain the purpose, the process and the assistance required from the site to support the evaluation. It is designed to build support for the on-site evaluation to follow by and set the parameters for information required to prepare the evaluation team. The team will validate the information already provided and gather additional needed information. This initial site briefing is scheduled to take one day.

Site data collection is the responsibility of the individual sites with guidance from the evaluation lead regarding required information. Ten work days are allocated to allow the site to collect the needed data.

Team preparation consists of reviewing the site provided information and, if permitted, probing the site for site configuration information. The evaluation team will tailor the interview instruments to the site. The interview instruments will focus on both the technical and organizational (policy, procedures, methodology) issues at the site. Team preparation usually takes 5 work days.

Onsite data collection consists of a series of interviews conducted by the team with organization personnel in peer groups or singly, in the case of the CIO, and technical reviews examining selected technologies installed in the organization. The onsite data collection usually takes 2 full days.

The data analysis by the team is conducted off-site after the conclusion of the site visit. It allows the team to do a thorough review of the material collected and to synthesize the findings and recommendations. Data analysis is scheduled for nine work days.

Feedback to the team consists of providing a detailed report on the results of the evaluation to the participants and to obtain feedback on what did and did not work from the site participant's perspective. This session normally takes a half day to complete.

Key Events:

- Site visit and initial briefings
- Enlist and prepare site coordinator
- Site prepares data to send to evaluation team
- Team tailors onsite data collection plan based on analysis of site provided information
- Conduct onsite data collection (interviews and technical review)
- Post-visit data analysis and briefing synthesis
- Feedback to site
- Feedback from site

Dependencies: Site selection and willing cooperation.

Schedule: This task consists of up to three instances of the evaluation process. Each evaluation is estimated to take approximately 30 working days from initial site briefing to briefing of final results

Composite Report on Evaluations

The evaluation team will prepare a summary report on the results of this series of evaluations. This report will not associate specific findings with identifiable sites but rather make generic observations about the observed state of information protection in the military healthcare systems. The report will be developed over the time period of the evaluations but not completed until after the conclusion of the final evaluation.

Key Events:

- Participate in site evaluations
- Prepare first draft
- Revise draft based on comments and additional data from site evaluations
- Prepare briefing to accompany release of report

Dependencies: Site selection and site evaluations

Schedule: The preparation of this report is estimated to take approximately 45 work days. This task may begin after completion of the first evaluation but will not conclude until after the completion of the third evaluation.

PROTOTYPE DEVELOPMENT

Developing the prototype system to be installed and operated during the demonstration will be based on the findings of the site evaluations. This work area is subdivided into system selection, system design, and prototype evaluation. A key component to successful prototype development and testing is the supporting task of emerging technology research. The design of a secure architecture will be directly related to the system selected to secure, appropriate design choices, and the integration of appropriate technology. Part of the prototype development process will be a thorough evaluation of the design and the demonstration prototype.

System Selection

One of the goals of this program is to demonstrate application of current and emerging technology to the protection of healthcare data. To accomplish that goal it will be necessary to apply information protection technology and associated organizational policies and procedures to a selected target system. The selection of that target system will be a crucial decision in this process. Identification of potential candidate systems will be an integral part of the site evaluation task. Selection of a target system should be based on support and resolution of the evaluation team's findings and recommendations.

Key Events:

- Identify preliminary system selection parameters
- Nominate potential candidate systems based on findings of evaluations
- Evaluate candidate systems against selection parameters
- Select target system

Dependencies: Site evaluations, system availability and configuration control.

Schedule: This task will commence with the site evaluations as members of the design team will be on the site evaluation team. A recommendation on an appropriate system to select for the demonstration is expected to be doable shortly after the conclusion of the final site evaluation.

Emerging Technology Research

Healthcare systems must be concerned with the availability, integrity and security of pertinent healthcare data. Open areas for potential research include understanding the challenges of integrating emerging technology associated with information protection (e.g. identification, authentication, authorization, encryption) into healthcare systems while insuring no degradation of availability to healthcare providers. An integral aspect of this supportive technology research is the development and population of a center where prototype security technology can be tested and demonstrated rapidly without impacting functional systems. To support this capability, a Rapid Prototype Facility is envisioned. This facility will consist of a test bed distributed across the members of this program, i.e., TATRC, ATI, LMES, and SEI. The combined power will be to rapidly and efficiently test emerging technology in a networked environment. Research into emerging technology will include three principle areas of research: simulating system architecture to validate expected performance; impact of design and technology choices on system performance characteristics; and building systems with known availability attributes (i.e. survivable systems). These research areas are core support pieces to the rest of the program and will be ongoing through the life of the program. The associated effort will be a combination of research, technical reports, demonstrations, and applied technology performed by participating team members.

Key Events:

- Develop research plan
- Design survivable architecture simulation
- Acquire and install support technology
- Develop white papers and technical reports on research results

Dependencies: Identification of technology and survivable architecture issues, findings and recommendations from site evaluations, system selection and design issues.

Schedule: This supporting task is ongoing. It will be initiated in mid-November 1998 and extend until program completion.

System Design

The system to be designed will be used to demonstrate the feasibility of securing a healthcare data system. System design will be based on findings and recommendations of the site evaluations. System designers will be participants with the evaluation teams. Design will include not only appropriate security technology but also recommended security policy, procedures and methods to support secure and available operations of the healthcare system.

Key Events:

- Design security components
- Develop security modules
- Acquire and install demonstration prototype for evaluation and validation of system performance

Dependencies: Site evaluation findings and recommendations, emerging technology research, acquisition and integration of appropriate technology.

Schedule: System design will formally begin after system selection and is expected to require 45 working days to reach initial prototype demonstration.

Prototype Evaluation

The prototype design will be evaluated by a team that is independent of the design team. The objective of the evaluation is to simulate the operations of the security components to understand the efficacy of the security components and the impact on the functional system. Testing will proceed from an audit of the design features, through a simulation of the secured system, to a demonstration of the secured system in a laboratory environment (pending feasibility of creating an emulation of the functional system).

Key Events:

- Develop test plan
- Test system security designs via scenario driven analysis by independent team of experts
- Fabricate simulation of system to validate system meets performance objectives
- Evaluate demonstration prototype in Rapid Prototype Facility

Dependencies: Emerging technology research in simulating secure environments, secure system design recommendations, rapid prototype facility capabilities.

Schedule: Development of the test plan may proceed before the system design is completed but should not commence prior to system selection since that may impact the system testing envisioned. The execution of the testing plan is estimated to take 20 working days from documentation of the design until completion of the design review.

DEMONSTRATION

The realization of the design and testing efforts will be a demonstrable systems that operates in a secure mode. This demonstration will include required technology applied and integrated with the functional system and the policies, procedures and methodologies required to operate the secured system. This work consists of acquiring the system components, integrating and installing those system components at the test beds, and operating those secured systems for a period of time to ensure proper operation of those systems.

Acquire and Install Test Beds

After the design has been validated, a detailed specification list of necessary system components tailored to the individual test bed sites will be developed. The components will be installed at the test bed sites by contractor personnel.

Key Events:

- System specifications including detailed list of necessary components
- Systems acquisition and integration
- System delivery and installation at test bed sites

Dependencies: System design, successful prototype evaluations, and system component availability.

Schedule: Acquisition and installation is estimated to take a total of 65 work days. Detailed system specifications to include required equipment list is estimated to require 10 work days to finalize. This activity may begin after the system has been designed and the prototype evaluated. System acquisition can begin after system design validation and is estimated to take 20 working days. We have allowed a period of 5 days for configuration testing prior to delivery on site but, based on system components, that may be reduced. Delivery to the sites should take no more than 5 working days and installation at each site is estimated to take 5 days per site for a total of 15 working days.

Operate Demonstration

Contractor personnel will operate the demonstration systems at the test bed sites as part of transitioning the technology and the procedures to the test bed sites. Part of the operation will include recommendation on appropriate site policy and procedures based on site evaluation findings and demonstration system design. The operation of the system will include hands-on training of site personnel in the proper configuration and operation of the system and onsite training to reinforce security awareness and oversight.

Key Events:

- Develop system operation policy and procedure guidance
- System operations on site
- Training in security awareness, oversight, and operations

Dependencies: System acquisition and installation, development of example policy and procedural guidance, system complexity.

Schedule: Development of recommendations on system operations policy and procedures can commence after the system selection and system design. That subtask is expected to take 15 work days. Systems operations to include training will be dependent on the system complexity but we estimate 45 work days to establish an initial operational capability and to operate and train on-site personnel.

TECHNOLOGY TRANSITION

One of the objectives of the program is to transition the technology, policies, and procedures to an operational environment. Establishing the test beds at operational sites and securing functional systems is a preliminary requirement to meet this objective. Other necessary requirements include incorporation of security policy and procedures into standard operating procedures and documenting lessons learned to improve the practices in healthcare information protection.

Key Events:

- Incorporation of policy and procedure recommendations
- Documentation of lessons learned
- Interface with other DoD agencies, i.e., DISC4, OSD(HA), OTSG

Dependencies: System design, acquisition, and installation; on-site system operations

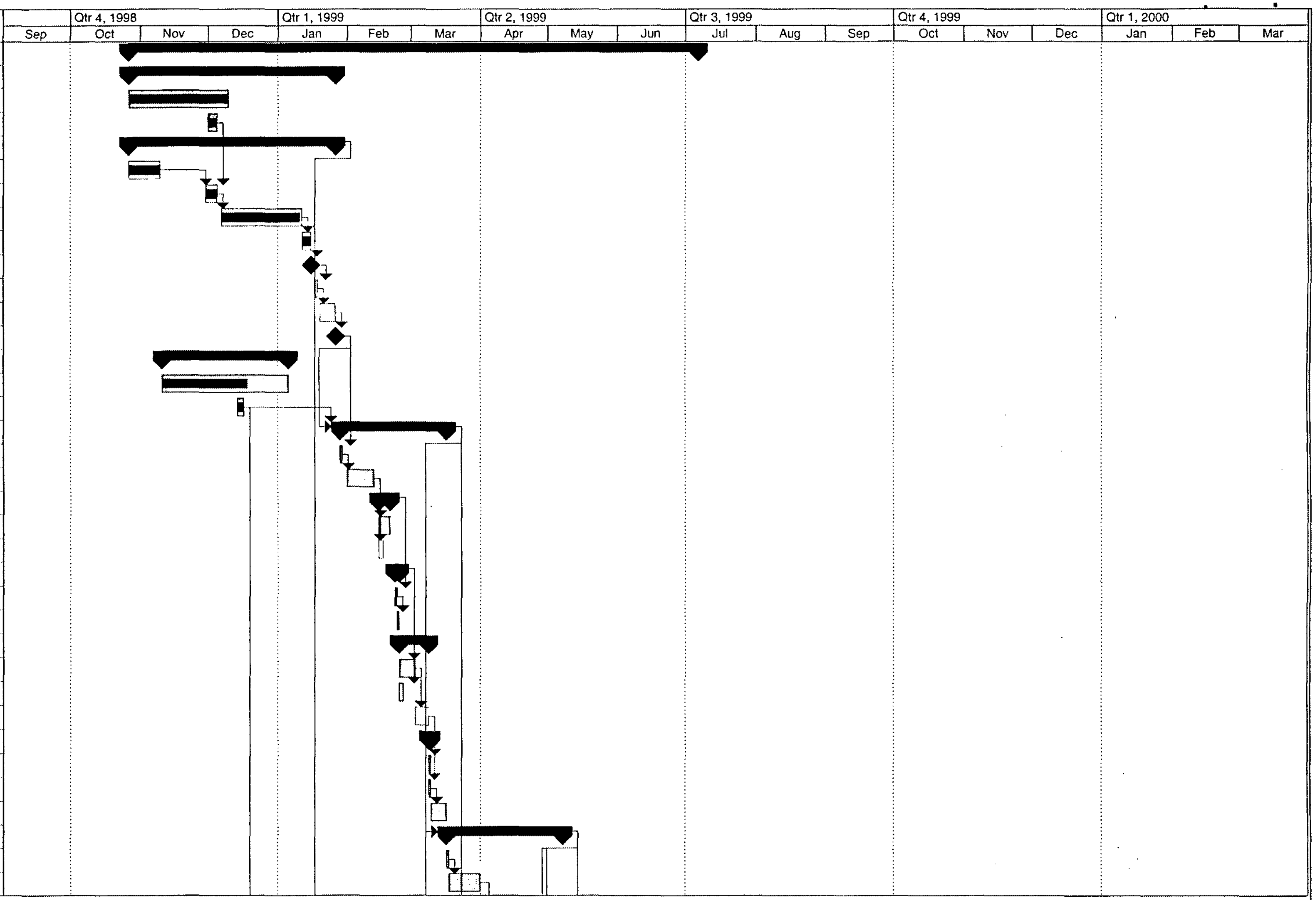
Schedule: Technology transition is an ongoing activity. Required reporting documents (quarterly, annual, and final reports), as well as other actions that will have impact on the transition of secure technology (composite site report, lessons learned, and interface with other DoD agencies) are scheduled in the WBS. This is an ongoing work area that spans the duration of the program.

WORK BREAKDOWN STRUCTURE

The anticipated work breakdown structure for this program is attached in the form of a Project Gantt chart. Schedule is notional at this time since the dependencies inherent in the program plan will impact the earliest dates that events may begin. The value of the Gantt chart is to understand the relative time anticipated for each of the work areas and the tasks that compose that work area, the sequencing of planned events and the dependencies associated with the events. This Gantt chart will be maintained as a living document as the program progresses and dependent events are resolved.

THIS PAGE INTENTIONALLY LEFT BLANK

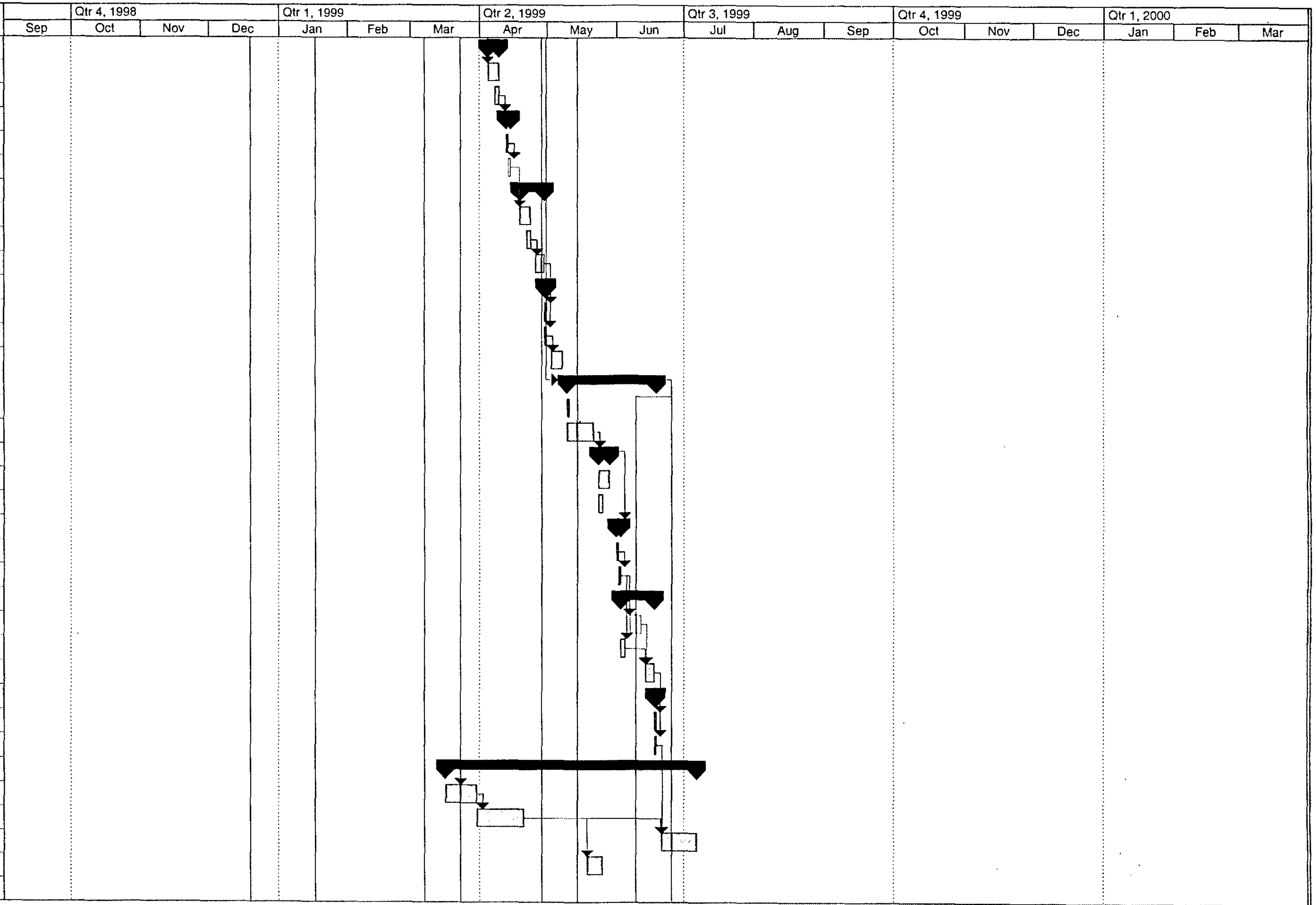
ID	WBS
1	**1**
2	**1.1**
3	1.1.1
4	1.1.2
5	**1.1.3**
6	1.1.3.1
7	1.1.3.2
8	1.1.3.3
9	1.1.3.4
10	1.1.3.5
11	1.1.3.6
12	1.1.3.7
13	1.1.3.8
14	**1.2**
15	1.2.1
16	1.2.2
17	**1.3**
18	1.3.1
19	1.3.2
20	**1.3.3**
21	1.3.3.1
22	1.3.3.2
23	**1.3.4**
24	1.3.4.1
25	1.3.4.2
26	**1.3.5**
27	1.3.5.1
28	1.3.5.2
29	1.3.5.3
30	**1.3.6**
31	1.3.6.1
32	1.3.6.2
33	1.3.7
34	**1.4**
35	1.4.1
36	1.4.2



Project: DHIAP Phase 1 v0
Date: Mon 10/22/01

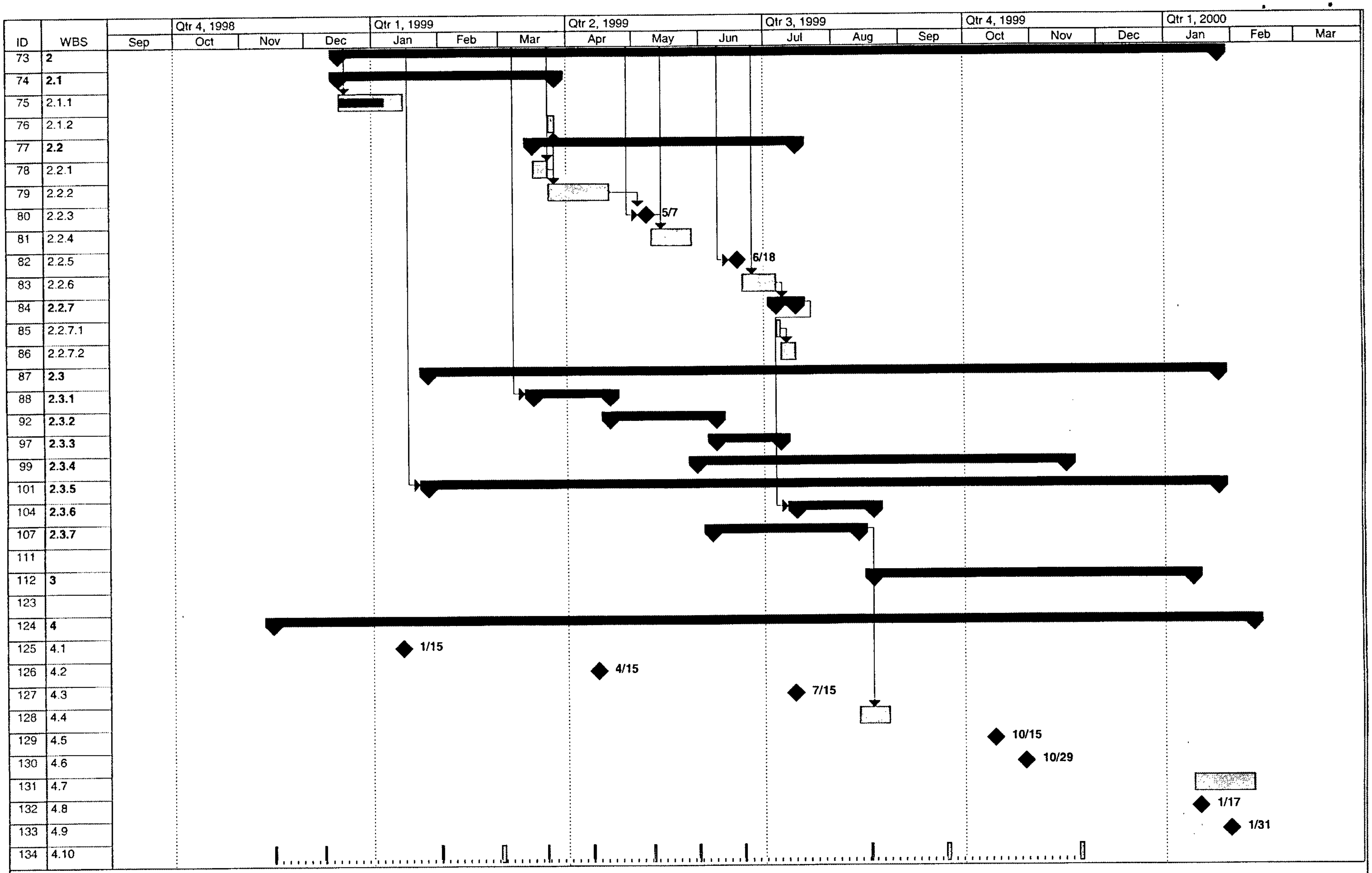
Task	▨	Summary	▬	Rolled Up Progress	▬	Deadline	⇩
Split	....	Rolled Up Task	▭	External Tasks	▭		
Progress	▬	Rolled Up Split	....	Project Summary	▨		
Milestone	◆	Rolled Up Milestone	◇	External Milestone	◇		

ID	WBS
37	**1.4.3**
38	1.4.3.1
39	1.4.3.2
40	**1.4.4**
41	1.4.4.1
42	1.4.4.2
43	**1.4.5**
44	1.4.5.1
45	1.4.5.2
46	1.4.5.3
47	**1.4.6**
48	1.4.6.1
49	1.4.6.2
50	1.4.7
51	**1.5**
52	1.5.1
53	1.5.2
54	**1.5.3**
55	1.5.3.1
56	1.5.3.2
57	**1.5.4**
58	1.5.4.1
59	1.5.4.2
60	**1.5.5**
61	1.5.5.1
62	1.5.5.2
63	1.5.5.3
64	**1.5.6**
65	1.5.6.1
66	1.5.6.2
67	**1.6**
68	1.6.1
69	1.6.2
70	1.6.3
71	1.6.4
72	



Project: DHIAP Phase 1 v0
Date: Mon 10/22/01

Task	▨	Summary	▬	Rolled Up Progress	▬	Deadline	⇩
Split	┈	Rolled Up Task	▨	External Tasks	▭		
Progress	▬	Rolled Up Split	┈	Project Summary	▨		
Milestone	◆	Rolled Up Milestone	◇	External Milestone	◆		



ID	WBS
73	**2**
74	**2.1**
75	2.1.1
76	2.1.2
77	**2.2**
78	2.2.1
79	2.2.2
80	2.2.3
81	2.2.4
82	2.2.5
83	2.2.6
84	**2.2.7**
85	2.2.7.1
86	2.2.7.2
87	**2.3**
88	**2.3.1**
92	**2.3.2**
97	**2.3.3**
99	**2.3.4**
101	**2.3.5**
104	**2.3.6**
107	**2.3.7**
111	
112	**3**
123	
124	**4**
125	4.1
126	4.2
127	4.3
128	4.4
129	4.5
130	4.6
131	4.7
132	4.8
133	4.9
134	4.10

Project: DHIAP Phase 1 v0
Date: Mon 10/22/01

Task	▨	Summary	■	Rolled Up Progress	■	Deadline
Split	....	Rolled Up Task	▨	External Tasks	□	
Progress	■	Rolled Up Split	....	Project Summary	▨	
Milestone		Rolled Up Milestone		External Milestone		

THIS PAGE INTENTIONALLY LEFT BLANK

Contract No.: DAMD17-99-C-9001

DEFENSE HEALTHCARE INFORMATION ASSURANCE PROGRAM (DHIAP)

Technical Development Plan
DHIAP Phase II

Version 4

December 2000

Prepared for:
U.S. Army Medical Research and Materiel Command
Fort Detrick
Frederick, Maryland 21702-5012

Change Log
for
Technical Development Plan – DHIAP Phase II

This section contains a history of changes made to the Technical Development Plan

DOCUMENT		*CONTEXT OF CHANGE*	
VERSION	PAGE(S)	DESCRIPTION	DATE
BASIS OF REVISION:	***Comments / Requests for Clarification in M. Younkins' 15 March 2000 letter***		
2	Title	Changed version number from "1" to "2."	16 Mar 00
2	Change Log	Added Change Log to document.	16 Mar 00
2	8, 27	Changed "Program Manager" references to "Senior Researcher."	16 Mar 00
2	13	Clarified wording in Task 2.4 to emphasize that SDRA training will include TATRC / Government trainees in addition to the four MTF-designated trainees.	16 Mar 00
2	13	Removed a Task 2.5 notation about site conduct of risk assessments: "There will be some assessment activities that the organization staff will perform and others for which they lack the necessary knowledge, skills, and abilities to perform."	16 Mar 00
2	14	Added a "vulnerability assessment tools" deliverable to Task 2.6.	16 Mar 00
2	15	Added "time and resource commitment" to RA Issues/Dependencies.	16 Mar 00
2	15	Clarified RA Deliverable describing turnover of reports/raw data in electronic format for inclusion in RIMR.	16 Mar 00
2	25	Added "DoD subscription" to BCA Issues/Dependencies.	16 Mar 00
2	25	Clarified BCA Deliverable describing turnover of reports/raw data in electronic format for inclusion in RIMR.	16 Mar 00
BASIS OF REVISION:	***Comments / Requests for Clarification from S. Labella on 23 March 2000***		
3	Title	Changed version number from "2" to "3."	24 Mar 00
3	Change Log	Modified Change Log to include statement on "Basis of Revision."	24 Mar 00
3	Travel tables and WBS throughout	To reflect that event timing is dependent on contract award date, date references were changed from a specific month/year to a relative date; in Travel tables, "Awd+n" is used ("Awd" indicates "contract award date;" "n" represents number of months after award); in the WBS, headings like "1st Quarter/Jan-Feb-Mar" became "Q1/1-2-3" (Q1/1 represents the month following contract award month).	24 Mar 00

DOCUMENT		*CONTEXT OF CHANGE*	
VERSION	PAGE(S)	DESCRIPTION	DATE
3	6-8, 22	Altered IPR emphasis. Modified Task 1.4, WBS, Deliverables, Travel events, and budget to reduce the planned periodic IPR meeting schedule to approximately three team meetings as needed, tentatively scheduled for planning purposes. The team meeting agenda will allow for a status update to COR and COR's staff.	24 Mar 00
3	7-8	Deleted the PI's Pre-Brief visits to TATRC for the Initial and Summary Command Briefings from the Travel Schedule and budget.	24 Mar 00
3	4, 7-8	Deleted the site recruitment travel from the Travel Schedule, the WBS, and budget.	24 Mar 00
3	7-8	Reduced number of conferences attended by Technical Management staff to three. Travel Schedule and budget were updated accordingly.	24 Mar 00
3	9	Added a description of the ATI Technical Staff's participation in Technical Management activities to ATI Participant Roles.	24 Mar 00
3	10, 17-18	To clarify KRM's participation in RA activities, added KRM to the RA Participants list and Participant Roles description (participation was included in RA Travel, WBS, and budget).	24 Mar 00
3	17	Added a description of the ATI Technical Staff's participation in RA activities to ATI Participant Roles.	24 Mar 00
3	17	Corrected typo "production" rather than "protection"	
3	18	To clarify ADL's participation in RA activities, added ADL to the RA Participant Roles description (participation was included in RA Participants, Travel, WBS, and budget).	24 Mar 00
3	27	To clarify participation of the ATI Technical Staff in BCA activities, added a description of their work to ATI Participant Roles (participation was included in BCA Travel, WBS, and budget).	24 Mar 00
3	32, 33	Deleted participation of ATI's Technical Staff in Simulation Capability activities from the ATI Participant Roles description, WBS, and budget. ADL and LMES removed from WBS and budget.	24 Mar 00
3	Appendix A	Revised WBS	24 Mar 00
BASIS OF REVISION: proposed changes to Risk Analysis technical project by SEI			
4	Title	Changed version number from "3" to "4."	Jan 01
4	Change Log	Modified Change Log…	
4	10	Deleted HOST, LMES, and KRM from the Participants List	17 Jan 01
4	12	Modified Major Activities list; added section on developing and delivering a SDRA tutorial, and renumbered the subsequent activities	17 Jan 01
4	14	Deleted "Prepare Risk Assessment Composite Report" WBS item from Major Activities list	17 Jan 01

DOCUMENT		*CONTEXT OF CHANGE*	
VERSION	PAGE(S)	DESCRIPTION	DATE
4	14	Deleted "Prepare Risk Assessment State-of-the-Practice Report" WBS item from Major Activities list	17 Jan 01
4	16	Modified Deliverables list and Schedule to reflect changes to Major Activities list.	17 Jan 01
4	17, 18	Modified travel table	17 Jan 01

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Program Description

The Defense Healthcare Information Assurance Program (DHIAP) Phase II will develop and apply tools and techniques that provide an evaluation of current networks and systems and address necessary doctrine, infrastructure, training, programmatic, and technology issues to improve information assurance for Army Medical Treatment Facilities (MTFs).

Organization of Technical Development Plan

This Technical Development Plan is organized into four major sections corresponding to the four projects in this phase of DHIAP. Each of the project sections includes the following:

- Brief statement of purpose for the project;
- Lead organization and primary participants;
- Background section providing the context for the project;
- Major activities related to the project;
  - The tasks and subtasks are described in detail in the associated narrative
  - Tasks are numbered to correspond to the associated Work Breakdown Schedule (WBS)
- Work Breakdown Schedule for the project;
- Issues and dependencies that might influence the successful completion of the activities;
- Deliverables from the project;
- Projected travel associated with the project (with potential travel for TATRC team members indicated to support planning for potential travel);
- Equipment required to support the project (directly or potentially);
- Participants in the project and their roles; and
- A projection of potential follow-on work, the Long-Term Vision for work in DHIAP Phase III.

Attached as Appendix A is a Gantt chart depicting the detailed Work Breakdown Schedule for all the projects.

Context

The following are brief abstracts of the three technical projects that compose Phase II of DHIAP:

Risk Analysis: The Risk Analysis effort will engage up to four MTF sites in assessing the risk and vulnerabilities to information systems at those sites. It will begin with DHIAP team-led expert assessments of potential vulnerabilities and risks at one of the sites. This initial effort will mature the tools and techniques in the risk assessment methodology being developed by the SEI as part of the OCTAVE project. These tools and techniques will then be transitioned to up to three two other sites via training and mentoring so that those sites, with expert coaching, can accomplish a site-led risk assessment. The ultimate goal is to develop the training, tools, and techniques that allow individual MTF sites to perform self-directed risk assessments, only engaging outside experts when necessary to supplement available staff.

Business Case Analysis: The Business Case Analysis work will provide the process and products associated with assessment of business criteria for implementing information system security and survivability technology. This work will address operational, personnel, policy and technology considerations that should be considered in implementation decisions. It will also define a methodology for performing the business case analysis that should be applicable to MTF sites and decision makers. MTF sites will be engaged in the effort to ensure that the work has a solid foundation in operational reality.

Simulation Capability: The Simulation Capability work is focused on early research and development of a simulation tool that will support research in mission survivability. The objective of this effort is to design and implement an automated simulation system that can be used to demonstrate, validate and depict problems and solutions in mission survivability for Army medical systems. During this project year the simulation tasks will produce and demonstrate the alpha version of the simulation system, prepare related documentation, continue research relevant to Army medical infrastructure survivability, and in conjunction with the Army, prepare a plan for follow-on use of the simulator.

1. Technical Management

As described above, DHIAP Phase II consists of three technical projects, each one integrated and interdependent in some way with the others. Managing the work includes: working with senior members of the project teams to plan tasks, schedules, and budgets; monitoring technical progress; managing project resources; reporting accomplishments and expenditures; and giving command and operational level briefings as requested by the Contracting Officer's Representative (COR).

Lead Organization

ATI

Participant

ADL

Background

The management effort began with development of this overall Technical Development Plan, a living document describing research goals, the plan for attaining those goals (tasks, resources, travel, equipment), products and deliverables, and external dependencies that may affect timing or results of the effort. Throughout the program, Technical Management will use the Plan as the basis of communication among team members and for monitoring progress of the program's work effort, timely preparation the indicated deliverables, and appropriate use of resources. As changes to the plan are needed, Technical Management investigates, reports, and justifies the need for the change and modifies the plan to reflect the change.

Major Activities

1.1 Initiate Phase II Work

1.1.1 Develop Technical Development Plan

The Technical Development Plan and its associated Work Breakdown Structure (WBS), attached as Appendix A to this plan, describe the schedule, resources, and plan for execution of each project. Together, they will be a living document, updated as needed (with approval of the COR and the COR's technical staff) to provide an accurate description of Phase II work.

1.1.2 Present initial command briefing on Phase II plans and schedule

Technical Management will develop a high-level briefing on the plans, schedule, and requirements for DHIAP Phase II. Preparation of the briefing material will include delivery to the COR and the COR's technical staff for review and feedback. The government will schedule the time and place for the briefing.

1.2 Recruit Sites

Based on decisions made in the February 16-18 DHIAP Phase II Kickoff Meeting, Technical Management will support TATRC's efforts to identify and recruit sites to participate in Phase II activities, including: the Risk Analysis project's assessments, the Simulation Capability's Simulation Advisory Group and MTF subject matter experts, and the Business Case Analysis project's research and potential demonstrations.

Technical Management will develop a high-level briefing on Phase II plans and support requirements for the leaders of Regional Medical Centers, operational MTFs, and critical Army and Tri-Service medical departments. The briefing will describe activities planned for Phase II and the role to be played by operational sites and their opportunities to participate in and benefit from the Risk Assessment, Business Case Analysis, and Simulation technical efforts. Briefings will be delivered to the COR and the COR's technical staff for review and feedback.

TATRC will arrange the times, locations, and audience of the Command Level Briefing. Technical Management will conduct the briefing and, as appropriate, key personnel from the Phase II technical projects will participate in the presentation or follow-on discussions. Following this presentation, potential sites to approach for participation will be identified. Technical Management will support TATRC in following up on leads, briefing the interested sites (via most effective means – currently planned as VTCs), and engaging the sites' support (see projects 2.2 and 3.2 for task-related details). A site selection coordination trip to TATRC to review progress and resolve any open issues has been scheduled.

1.3 Manage DHIAP Activities

1.3.1 Manage DHIAP technical work

Technical Management will oversee execution of all DHIAP Phase II work. This began with leading the team effort to develop the project's Technical Development Plan, and will continue with monitoring the progress of the project work efforts, production of deliverables, and use of resources. Management will use the Technical Plan as a communication tool among team members and will modify the Plan and WBS documents as project changes occur.

Where deviations from the Technical Plan are observed or are deemed necessary, Technical Management will work with project leaders to identify reasons and define needed action; the need for the change will be reported and justified in the next scheduled periodic review with the COR and the COR's technical staff. Periodic updates at TATRC on program progress and issues may be required.

1.3.2 Facilitate project and cross-project activities

Throughout Phase II, Technical Management will coordinate team activities and facilitate collaboration among members of the distributed team. This includes providing support as appropriate for electronic file transfer, electronic mail, software installation and use, and other forms of technical assistance. Technical Management will collect project-level raw and analyzed data, format it, and deliver it to the COR and the COR's technical staff.

1.3.3 Provide regular project reporting

1.3.3.1 Monthly Reporting

Technical Management will prepare monthly summaries of project status (except at quarter-end when the Quarterly Report will be prepared instead). The monthly reports will describe:

- Project activity and accomplishments during the period;

- Issues;
- Changes to the proposed plan; and
- Use of staff and other cost-related resources. (Note that labor news will be reported by organization, rather than by task or project, due to restrictions in company accounting/reporting capabilities.)

Monthly reports will be submitted in electronic form.

1.3.3.2 Quarterly Reporting

Technical Management will continue to prepare the Quarterly Report at the end of each program quarter. The report will comply with the Army's formatting requirements, providing:

- Background;
- Current staff;
- Contract expenditures;
- Administrative and logistical matters;
- Technical progress;
- Planned activities; and
- Issues

1.3.3.3 Provide Meeting Minutes and Trip Reports

Meeting Minutes

Technical Management will prepare, or assure preparation of, minutes of meetings that have impact on Phase II responsibilities, deliverables, or schedule. Minutes will be electronically submitted to the COR and the COR's technical staff not later than seven working days following the meeting. They will detail:

- Date and purpose of the meeting;
- Point of contact for the meeting,
- Attendees;
- Findings and conclusions;
- Action items; and
- Recommendations resulting from the meeting.

Where appropriate, electronic copies of briefings or papers related to the meeting will also be provided.

Trip Reports

Technical Management will prepare, or assure preparation of, trip reports and submit them electronically to the COR and the COR's technical staff not later than seven working days following completion of travel. Reports will detail:

- Date, purpose, and destination of travel;
- Point of contact for the visit;
- Attendees;
- Activities and conclusions; and
- Recommendations resulting from the visit.

Where appropriate, electronic copies of briefings or papers related to the visit will also be provided.

1.4 Conduct Team IPRs/Command Briefings

Interim progress reviews (IPRs) will be held by the DHIAP Team as required to assess progress, coordinate joint activities, revise plans as necessary, etc. Where appropriate, occurrence of these meetings will be planned to coincide with the opportunity to provide input to the COR and the COR's technical staff on work accomplished, cost, schedule, resources, quality, customer satisfaction, subcontractor relationships, and risks; the time and place will be closely coordinated with the COR. For planning purposes, tentative dates and locations for these team meetings have been identified as: the first at SEI in Pittsburgh PA in June 2000, the second conducted by VTC/teleconference in October 2000, and a third in Charleston SC in January 2001.

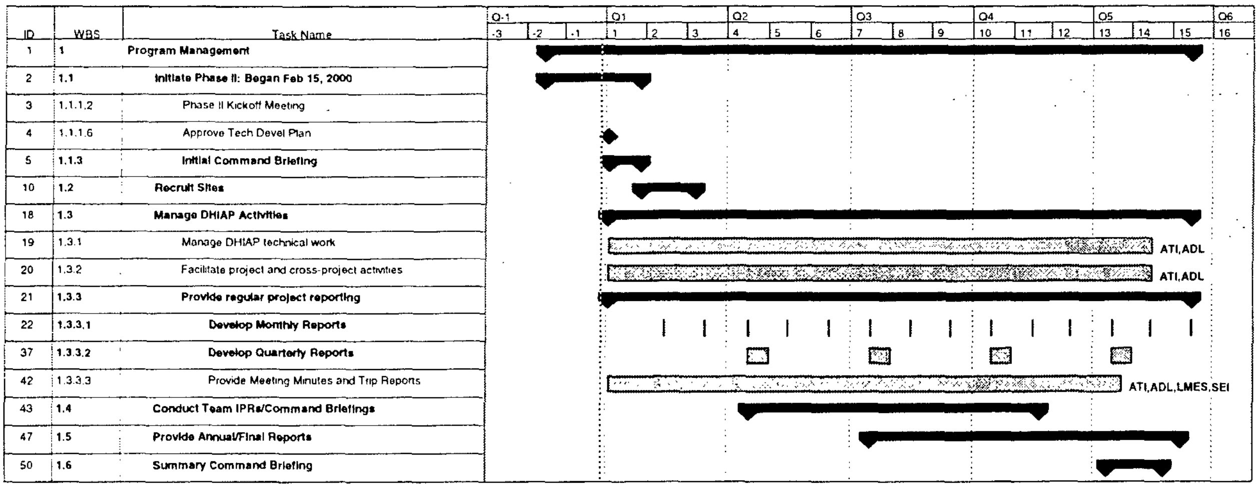
1.5 Provide Annual/Final Reports

Technical Management will provide an Annual Report of DHIAP Phase I and II accomplishments during the year ending in mid-October (the anniversary of the initial DHIAP contract), formatted to comply with the Army's reporting requirements. Unless superceded by continuation of DHIAP into a subsequent phase, Technical Management will provide a DHIAP Final Report at the end of Phase II that details accomplishments and lessons learned over the life of the project.

1.6 Present Final Command Briefing

Technical Management will prepare, deliver for review by the COR and the COR's technical staff, and present a final command briefing to summarize work accomplished during DHIAP Phase II.

Schedule



ID	WBS	Task Name
1	1	**Program Management**
2	1.1	**Initiate Phase II: Began Feb 15, 2000**
3	1.1.1.2	Phase II Kickoff Meeting
4	1.1.1.6	Approve Tech Devel Plan
5	1.1.3	**Initial Command Briefing**
10	1.2	**Recruit Sites**
18	1.3	**Manage DHIAP Activities**
19	1.3.1	Manage DHIAP technical work
20	1.3.2	Facilitate project and cross-project activities
21	1.3.3	**Provide regular project reporting**
22	1.3.3.1	**Develop Monthly Reports**
37	1.3.3.2	**Develop Quarterly Reports**
42	1.3.3.3	Provide Meeting Minutes and Trip Reports
43	1.4	**Conduct Team IPRs/Command Briefings**
47	1.5	**Provide Annual/Final Reports**
50	1.6	**Summary Command Briefing**

Figure 1 - WBS Gantt Chart for Technical Management Effort

Figure 1 above indicates the activities, planned timeframes, and participants of the major activities of the Technical Management effort.

Issues / Dependencies

- An early external dependency in Phase II is the requirement to establish a mutually beneficial working relationship with operational medical centers and the Simulation Advisory Group. The sites who will participate in the four Risk Analyses and the Business Case Analyses must be enrolled in the first months of Phase II.

Deliverables

1. Detailed Technical Development Plan and WBS
2. Command Briefing on plans and schedule for DHIAP Phase II (the government will schedule the time and place for this command level review)
3. Command and operational level briefings to recruit MTFs and designated individual experts as project participants (the government will schedule the time and place for this command level review)
4. Monthly and Quarterly Reports and, on request, IPR on project status and accomplishments
5. Minutes of significant project meetings, with electronic copies of briefings or papers related to the meeting
6. Trip Reports, with electronic copies of briefings or papers related to the event
7. Annual Report detailing accomplishments in the past year
8. Final Report detailing accomplishments and lessons learned over the life of the program
9. Command Briefing on DHIAP accomplishments (the government will schedule the time and place for this command level review)

10. Various DHIAP-related attendance/presentations (TBD) at professional conferences and at meetings arranged by TATRC

Travel

Travel required to support Technical Management responsibilities is summarized in the following list. Table 1 at the end of the list provides additional information about the participating organizations and number of travelers for each event.

- Phase II Kickoff Meeting: The Phase II team visited Charleston SC to work with TATRC on revising plans for Phase II activities and to make the decisions necessary to draft a Technical Development Plan for Phase II.
- Initiate DHIAP Phase II Work: The ATI PI will visit Ft. Detrick to deliver the Command Brief.
- Recruit Sites: ATI (with leader from the Risk Assessment) will brief up to eight sites on the RA and BCA projects and benefits to the site of participation. The site briefings will be conducted as much as possible via video teleconferencing capabilities. A trip or VTC with TATRC to ensure progress on site selection and to resolve any open issues is included in the planning.
- Interim Program Reviews (IPRs): The ATI PI will plan, organize, and lead IPRs. For planning purposes, tentative dates and locations include an IPR at SEI in Pittsburgh PA in June 2000, a VTC/teleconference in October 2000,and one in Charleston SC in January 2001.
- TATRC Meetings: The ATI PI and senior researcher will conduct or attend meetings with TATRC as needed for program communications and/or to present to military groups brought together by TATRC in the Washington D.C. area. For planning purposes, two meetings at Ft. Detrick were included in the travel estimates. These meetings will be arranged with the DHIAP COR's and the COR's representatives in advance of any travel.
- Summary Command Briefing of Phase II Work: The ATI PI will visit Ft. Detrick to deliver a Command Brief summarizing the work accomplished in Phase II.
- As DHIAP leader: The DHIAP PI and appropriate senior staff will visit Oak Ridge TN and Pittsburgh PA for interim review of efforts to apply the Business Case Analysis methodology developed in the BCA project, and review training and materials developed for the RA project's Self-Directed Risk Assessments.
- To publicize DHIAP efforts, compare DHIAP activity with other advanced research efforts, and gain knowledge relevant to DHIAP initiatives: The DHIAP PI, and/or ATI senior researcher and technical staff will attend selected, DHIAP-related professional conferences. For estimating purposes, travel estimates identify three conferences. They are:
  - Computerized Patient Record Institute (CPRI) annual conference in Washington D.C.
  - American Telemedicine Association (ATA) annual conference (DHIAP poster session accepted for May 2000 conference) in Phoenix AZ
  - National Information Systems Security annual conference in Baltimore MD

Projected travel is depicted in Table 1 below. Note that the Team Members column indicates "(TATRC)" for trips involving subjects that the TATRC team members may wish to participate in. This information is provided for TATRC's budgeting of potential travel.

Month	To	Reason	Team Member(s)	Contractor Travelers
Feb-00	Charleston, SC	Phase II Kickoff / Planning	ATI, ADL, SEI, LMES, HOST, KRM, (TATRC)	5
Awd + 1	Washington, DC	Initial Command Brief	ATI, SEI, (TATRC)	4
Awd + 2	Ft. Detrick, MD	Site Selection Coordination	ATI, SEI, (TATRC)	3
May-00	Phoenix, AZ	ATA Conference	ATI	1
Awd + 4	Pittsburgh, PA	IPR #1	ATI, SEI, ADL, LMES, HOST, KRM, (TATRC)	6
Jul-00	Washington, DC	CPRI Conference	ATI	2
Awd + 5	Ft. Detrick, MD	TATRC Coordination Meeting	ATI	2
Oct-00	Baltimore, MD	NISSC Conference	ATI	1
Awd + 8	Pittsburgh, PA	Team Coordination Meeting	ATI, SEI	2
Awd + 8	VTC/Telecon	IPR #2	ATI, SEI, ADL, LMES, HOST	0
Awd + 9	Oak Ridge, TN	Team Coordination Meeting	ATI, LMES	2
Awd + 9	Ft. Detrick, MD	TATRC Coordination Meeting	ATI	2
Awd + 11	Charleston, SC	IPR #3	ATI, SEI, ADL, LMES, HOST, (TATRC)	5
Awd + 14	Ft. Detrick, MD	Summary Command Brief	ATI, (TATRC)	2

Table 1 - Projected Travel for Technical Management

Participant Roles

This project will be led by ATI, augmented as required by ADL.

- **ATI** will provide a Senior Researcher and PI to perform Technical Management tasks including: overall coordination, scheduling and monitoring of Phase II activities; reporting and presentation of status and accomplishments; and writing final editing, and submission of program deliverables. ATI Technical Staff (i.e., Senior Researcher, Systems Analyst, and/or Researcher) will provide collaboration support for the DHIAP Team, including electronic file transfer, electronic mail, software installation and use, and other forms of technical assistance. In addition, as needed, they will support Technical Management's activity to define appropriate electronic formats for data the collected during Risk and Business Case Analysis project activities.

- **ADL** will provide program management and monitoring expertise to support: program planning; scheduling of activities and milestones; forecasting and making recommendations on funding and funding changes; preparation and execution of program reviews; assistance in daily tasks (e.g., resource tracking, action item monitoring, program status reporting, and preparation of deliverables); and preparation of Monthly Financial Report, Monthly and Quarterly Technical Status Reports, Annual Summary Report, and the Final Program Report.

2. Risk Analysis

The DHIAP Team will develop risk assessment tools and methodology based on the SEI's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) project and conduct a series of risks assessments for healthcare information systems at MTFs selected by the government. This effort will result in piloting a Self-Directed, DHIAP Team-mentored Risk Assessment at selected MTFs.

Lead Organization

Software Engineering Institute (SEI)

Participants

ATI, ADL

Background

In today's medical environment, virtually all medical information is stored electronically. Because networked computing is so common in the medical community, legitimate users have greater access to information than ever before. Unfortunately, this availability also exposes the medical community to a variety of new threats that can have impact on the confidentiality, integrity, and availability of information. Information assurance has become a great concern to the medical community. MTFs need a better way of understanding their information risks and creating new strategies for addressing those risks.

A systematic approach to assessing information security risks and developing an appropriate protection strategy is a major component of an effective information security program. By adopting a systematic approach, MTFs can better understand their current security posture and use it as a benchmark for improvement. The Self-Directed Risk Assessment will enable medical organizations to systematically identify risks to information, prioritize those risks, and take appropriate steps to manage them.

The Self-Directed Risk Assessment (SDRA) is intended to be an effective enterprise-wide evaluation of information security risk that will comprise the following:

- **Organizational Evaluation** – Examines key areas of expertise within the organization to identify information assets, threats, security requirements, current protection strategy, and organizational vulnerabilities
- **Information Infrastructure Evaluation** – Examines the key operational components of the information infrastructure for weaknesses that can lead to unauthorized action (technology vulnerabilities)
- **Analysis of Risk** – Analyzes the information generated by the organizational and information infrastructure evaluations to identify risks to the enterprise and to develop a protection strategy for addressing the highest priority risks

The Self-Directed Risk Assessment is an applied research project that leverages the development and delivery experience of SEI-DHIAP Team with DHIAP Phase I's Information Security Evaluation (ISE), and SEI development and delivery work in risk management for software engineering projects accomplished at the SEI. The SEI is currently working to integrate its risk identification and assessment techniques with its ISE method to create an information security risk evaluation methodology known as OCTAVE. The methods proposed for the DHIAP Phase II risk assessments are based on this research foundation.

Major Activities

2.1 Design/Develop OCTAVE Tools and Methodology

The DHIAP Team will develop the OCTAVE risk assessment methodology, along with appropriate supporting tools and techniques. The goal of this activity is for MTF sites and other military health-related organizations health information systems to be able to determine risks in the physical and electronic transmission and storage of sensitive healthcare information.

The methodology developed will be comprised of three components: an organizational evaluation, an information infrastructure evaluation, and an analysis of risk. Prototype versions of method artifacts (guidelines, templates, and checklists) will be developed.

2.2 Recruit/Select Sites for OCTAVE-based Risk Assessment

The DHIAP team will prepare an MTF-oriented briefing on the advantages and impact of a risk assessment. This briefing will be presented to MTF sites designated by TATRC, based on briefing schedules to be coordinated with TATRC and the sites, with the intent of enlisting MTF sites willing to pilot the tools and techniques. Potential participant sites will be identified by multiple means: as a result of the initial Command briefing relating the entire DHIAP Phase II effort, based on personal knowledge of suitable MTF sites, and by preliminary contact with TATRC and/or DHIAP team members.

Two types of pilot sites will be selected: sites willing to support an expert-led risk assessment, and sites willing to support an expert-mentored, self-directed risk assessment. Ideally, the selection process will identify multiple sites as potential candidates for each type of assessment. TATRC will select two sites for an expert-led risk assessment and two sites for an expert-mentored, self-directed risk assessment from the candidate sites willing to participate.

2.3 Conduct DHIAP-led Risk Assessments at One MTFs

The DHIAP team will pilot and refine the OCTAVE tools and techniques during the course of conducting one DHIAP Team-led Risk Assessments at selected MTFs. The assessment will consist of an organizational and information infrastructure evaluation, an analysis of risk, and delivery of an exit briefing presenting the results of the assessment to the site.

The site engagement will require multiple visits. These visits will include a preliminary visit to the site by the team to plan the engagement and to set expectations and commitments, and subsequent site visits to work with site personnel to identify potential threats, to evaluate the organizational influences, and to evaluate the information infrastructure. These initial series of visits will accomplish the raw data collection for subsequent analysis and action planning. The site piloting the team-led risk assessment will complete these phases of the risk assessment prior to being engaged in the risk analysis phase.

Following initial analysis of the results and further development and refinement of the appropriate tools, the pilot site will engage in DHIAP Team-led analysis of the threat/risk posture and development of a site-specific risk mitigation plan. Results of the risk analysis will be briefed to the site commander and designated staff for their action. The result of the site engagement will be that on-site personnel are equipped to begin execution of the risk abatement plan that they developed. Assessment results and raw data will be provided to the sites participating and to TATRC for inclusion in the Risk Information and Management Resource (RIMR).

2.4 Develop/Deliver SDRA Tutorial [NEW PARAGRAPH]

The OCTAVE team will develop a half-day tutorial on the Self-Directed Risk Assessment methodology. This tutorial will serve as an awareness vehicle for potential MISRT teams. The tutorial will be part of the regional MISRT (Medical Information Security Readiness Team) Training Seminars to be offered in the first quarter of 2001. Representatives from the OCTAVE team will deliver the tutorial in support of the following seminars:

January 26,2001	Bethesda, MD
January 29, 2001	Chesapeake, VA
February 12, 2001	San Antonio, TX
March 26, 2001	Augusta, GA

TATRC personnel will observe one or more of the tutorial deliveries at the seminars detailed above. The OCTAVE team will provide the TATRC representatives with the tutorial materials and sufficient support to allow TATRC personnel to be able to deliver the tutorial at the remaining MISRT seminars.

2.5 Develop/Deliver SDRA Training

In conjunction with and as a result of the experience gained during the DHIAP Team-led Risk Assessments, the SEI will develop training to enable MTF staff members (MISRT teams) to manage a Self-Directed Risk Assessment process. The training will be delivered to the MISRT team representing each of the MTF sites participating in the pilot of the Self-Directed Risk Assessment. In addition to participants selected by MTFs (the MISRT team), training participants will also include government-designated observers such as TATRC technical staff.

A facility has been identified as the first Self-Directed Risk Assessment site. The OCTAVE team will deliver training to support the SDRA at the identified site. Following scheduling of the SDRA training, up to three additional sites will be approached for involvement in a SDRA pilot (one of these teams will be the site analysis team involved in the Expert-Led Risk Assessment). These sites will attend the SDRA training and will conduct their assessments in parallel with the training site. The training will be delivered at the identified MTF site or at a location convenient to all sites participating in the SDRA pilot.

Following the delivery of the SDRA training, the OCTAVE team will use the lessons learned to refine and package the SDRA training materials.

2.6 Mentor Self-Directed Risk Assessments at two MTFs

The pilot Self-Directed Risk Assessments will be a continuation of the training in the methodology. Teams representing up to four sites will receive training on the Self-Directed Risk Assessment. Following the training, the selected sites will conduct their Self-Directed Risk Assessments in parallel, with the assistance of the DHIAP team mentors who developed the methodology and conducted the training. The risk assessments will be directed by the site-selected personnel (the MISRT teams consisting of military, civilian, and/or contractual personnel) who have been trained in the Self-Directed Risk Assessment methodology. The DHIAP Team mentors will provide guidance to up to three sites during the conduct of the assessments. The DHIAP team mentors will provide dedicated, targeted support to the MISRT/analysis team conducting the SDRA. The process used during these assessments will incorporate the lessons learned from the first DHIAP-led risk assessment.

The goal of using MTF staff in various tasks of the Risk Assessments is to create a method where an organization manages and directs a risk assessment for itself. This does not imply that the MTF must perform all activities internally; rather, the organization must be engaged in directing the activities, whether conducted by its staff or an outside organization. The site's personnel will decide if and when they need to draw upon external resources or expertise to complete the assessment. In the case of these pilots, the DHIAP team may be available to provide external resources or expertise to act under the direction of the site personnel. DHIAP Team expertise will be used to supplement the pilot site's MISRT/analysis team when deemed appropriate by both the DHIAP and site teams. Assessment results and raw data from the Self-Directed Risk Assessment will be provided to TATRC for inclusion in the Risk Information and Management Resource (RIMR).

2.7 Provide Method/Training/Templates/Checklists to RIMR (Risk Information and Management Resource)

As a result of the research and development effort for the Self-Directed Risk Assessment, a number of tools supporting the process will be developed and integrated. Where possible, the development activity will leverage known and effective tools. Other tools to support the method will have to be created. The following types of tools will be provided to TATRC for inclusion in the RIMR:

- Training materials;
- Method guidelines for conducting an assessment;
- Templates required by the process; and
- Checklists required by the process.

The OCTAVE team will develop a Self-Directed Risk Assessment Implementation Guide. The Implementation Guide will consist of the method guidance for the analysis team conducting the assessment, as well as the templates, checklists, surveys, and other artifacts required by the methodology. A beta version of the Implementation Guide will be provided to TATRC prior to the MISRT Training Seminars and to the initial training for the Self-Directed Risk Assessments.

Following the training and mentoring for the Self-Directed Risk Assessments, the OCTAVE team will refine the SDRA training materials based on lessons learned prior to delivery of these materials to TATRC.

In addition, vulnerability assessment tools (to include shareware that would run diagnostic software to identify and document risks and vulnerabilities at the sites) will be provided and identified.

Issues / Dependencies

- Engagement of RA/SDRA sites: The government will identify sites willing to participate in a pilot of the risk assessment methodology. The DHIAP Team will be prepared to brief MTF leadership regarding the RA/SDRA process and to assist in engaging at least four MTFs for participation in the pilot efforts.
- Permission to release site-specific data to RIMR: As a prerequisite to selecting a site for inclusion in a risk assessment pilot, the DHIAP Team will obtain the site's permission for release of identifiable risk and vulnerability information to TATRC for use in populating RIMR.
- Site availability: The schedule for the development of the Self-Directed Risk Assessment will be contingent upon timely recruitment of MTFs to participate in pilot deliveries.
- Time and resource commitment: The SEI and ATI DHIAP Teams will outline in detail for TATRC the expected MTF/Government time and resources required to fulfill a commitment for RA/SDRA process before TATRC solicits MTF/Government participation.
- Lead time to assure staff availability at the site: The availability of a site's staff and the lead time required by the sites to prepare for participation could affect the development schedule.
- Information sharing with the Business Case Analysis team: The Risk Analysis Team will consider using the draft Business Case Analysis Methodology provided by the BCA team in making decisions about types of information to be collected during Risk Assessments. In addition, the Risk Analysis Team will provide RA-collected information relevant to the Business Case Analysis studies to that team for use in their work.
- Effect of unknowns on schedule/scope of an R&D effort: The development of the Self-Directed Risk Assessment is a research and development task. The objective of the effort is to develop, test and refine a self-directed information security evaluation. As in any research project, unknowns that may affect the schedule and/or scope of the project may exist.

Deliverables

1. All reports and raw data resulting from Task 2 in electronic format suitable for inclusion in RIMR (Reports will be provided to TATRC in MS Word format, and all raw data collected during the course of work groups and interview sessions will be provided using generally available, affordable tools such as MS Access, Excel, or Word as appropriate to the type of information collected. The initial project task for "development of the methodology" will include definition of the data to be collected and the tools to be used in recording it for RIMR.)

2. Exit briefings for each MTF involved in an Expert-Led Risk Assessment assessed, including documentation of observations and recommendations

3. Health information assurance Self-Directed Risk Assessment method with associated risk identification and abatement tools and training materials; in the form of the OCTAVE method implementation guide and associated training materials.

4. Training for military, civilian and/or contractor personnel selected by US Army in use of the Self-Directed Risk Assessment tools and methodology. (This training includes mentored execution of the Self-Directed Risk Assessment at the designated MTF.) Execution of the Self-Directed Risk Assessment methodology will include assistance in preparation and delivery of the exit briefing to the MTF and the report of findings

Schedule

Figure 2 below indicates the activities, planned timeframes, and participants of the major activities of the Risk Analysis effort.

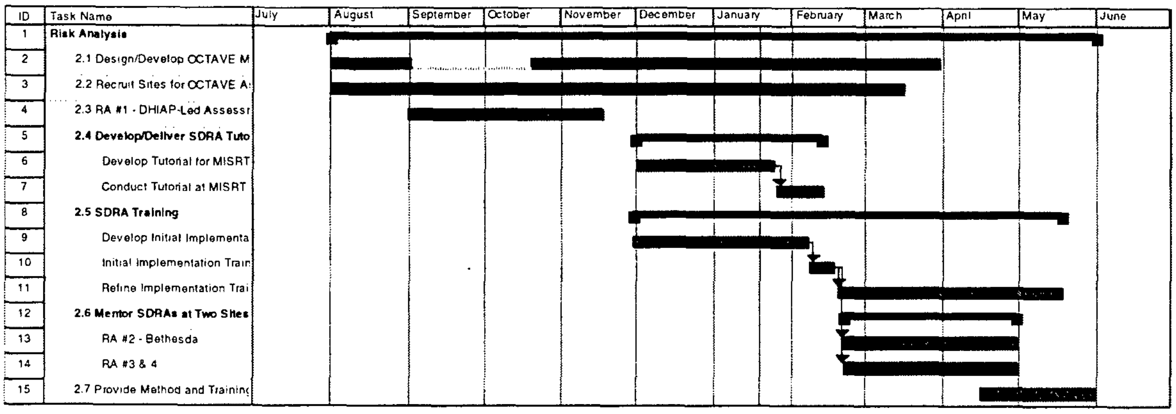


Figure 2 - WBS Gantt Chart for Risk Analysis

Travel

Most of the work of this project involves conducting risk assessments at military MTFs. Note that sites identified in the projected travel descriptions below are listed for budget estimation purposes only. The actual sites will be identified by TATRC and by the sites themselves by committing to the pilot effort. Travel to support the MISRT Training Seminars will not be funded by the DHIAP II effort.

- Following site identification, travel will first be required to conduct organizational and information infrastructure evaluations at the sites selected for the expert-led risk assessments. Travel estimates for this activity include pre-site visits to Norfolk VA, followed by visits to the same locations to perform the expert-led risk assessments. The team will meet in Pittsburgh to complete refinement of OCTAVE Phase III plans and materials, then travel again to Norfolk to conduct the analysis of risk and to develop/conduct the site Exit Briefings.

- Travel for the self-directed risk assessments will begin with travel to develop and deliver the training materials for the Self-Directed Risk Assessment. (For the purpose of cost estimation, MTFs at Bethesda MD, Augusta GA and Savannah GA have been selected as the potential mentored SDRA sites; however, until a final selection has been made, travel to them has been estimated separately to two distinct geographic locations SDRA training will be delivered at a central site or at a location convenient to all participating SDRA pilot sites.
- Travel to mentor the Self-Directed Risk Assessment will involve multiple, dedicated visits to the training site. Joint visits to the other two sites will be scheduled to mentor activities at both sites while conducting the Self-Directed Risk Assessment.

Projected travel is depicted in Table 2 below. Note that the Team Members column indicates "(TATRC)" for trips involving subjects that the TATRC team members may wish to participate in. This information is provided for TATRC's budgeting of potential travel.

Month	To	Reason	Team Member(s)	Contractor Travelers
Awd + 3	Norfolk, VA	Site 1: Initial Site Brief	ATI, SEI, HOST, (TATRC)	5
Awd + 3	Norfolk, VA	Site 1: Site Brief	ATI, SEI, HOST, (TATRC)	5
Awd + 4	Norfolk, VA	Site 1: Phase I-II Site Assessment, Trip #1	ATI, SEI, LMES, HOST, (TATRC)	6
Awd + 4	Norfolk, VA	Site 1: Phase I-II Site Assessment, Trip #2	ATI, SEI, LMES, (TATRC)	5
Awd + 4	Norfolk, VA	Site 1: Phase I-II Site Assessment, Trip #3	SEI, (TATRC)	3
Awd + 6	Pittsburgh, PA	Phase III Analysis & Assessment	ATI, HOST, SEI, (TATRC)	2
Awd + 7	Norfolk, VA	Site 1: Phase III Risk Analysis	ATI, SEI, (TATRC)	5
Awd + 8	Norfolk, VA	Site 1: Phase III Exit Brief	ATI, SEI, (TATRC)	5
Awd + 8	Pittsburgh, PA	Self Directed Risk Assessment (SDRA) Training Review	ATI, SEI, (TATRC)	2
Awd +11	Bethesda, MD	Training Development / Site Liaison	SEI, (TATRC)	3
Awd + 11	Augusta, GA and Savannah, GA	Training Development / Site Liaison	ATI, SEI, (TATRC)	4
Awd + 11	Bethesda, MD	Deliver SDRA Training	ATI, SEI, ADL, (TATRC)	6
Awd + 11	Bethesda, MD	Guide/Mentor Site 2 MTF Staff During SDRA (Bethesda)	ATI, SEI, (TATRC)	3
Awd + 12	Savannah, GA	Guide/Mentor Site 2 MTF Staff During SDRA (Bethesda)	SEI, (TATRC)	2

Month	To	Reason	Team Member(s)	Contractor Travelers
Awd + 12	Bethesda, MD	Guide/Mentor Site 2 MTF Staff During SDRA (Bethesda)	SEI, (TATRC)	2
Awd +12	Bethesda, MD	Guide/Mentor Site 2 MTF Staff During SDRA (Bethesda)	SEI, (TATRC)	2
Awd + 11	Savannah/Augusta GA	Guide/Mentor Site 3&4 MTF Staff During SDRA	ATI, SEI, (TATRC)	3
Awd + 12	Savannah/Augusta GA	Guide/Mentor Site 3&4 MTF Staff During SDRA	SEI, (TATRC)	2
Awd + 12	Savannah/Augusta GA	Guide/Mentor Site 3&4 MTF Staff During SDRA	SEI, (TATRC)	2
Awd +12	Savannah/August GA	Guide/Mentor Site 3&4 MTF Staff During SDRA	SEI, (TATRC)	2

Table 2 - Projected Travel for Risk Analysis

Equipment

The equipment requirements to support the Risk Analysis work consist of three portable laptop computers with the ability to run diagnostic software to identify and document risks and vulnerabilities at the sites. Two of the laptops will be used primarily by SEI and one will be used primarily by ATI. All of the laptops will be available for use by other team members involved in this project. An external monitor, a network card, and Linux software will support remote analysis probes on the selected sites. Portable printers will provide the analysis team with the necessary capability for on-site production of documentation. The equipment recommended and the estimated costs are presented in Table 3.

Risk Analysis Equipment			
Description	**Quantity**	**Unit Cost**	**Cost**
Dell Inspiron 3800 Notebook,, Pentium III, 650 MHz • *512MB, SDRAM, 2 DIMMs* • *18GB Ultra ATA Hard Drive* • *Modular CD-R/RW Drive* • *Canon BJC-50 Bubble Jet Portable Printer*	*2*	*$5,373*	*$10,746*
Dell Latitude CPx Notebook, Pentium III, 500 Mhz • *128MB, SDRAM,* • *12GB Hard Drive* • *CD-R/RW Drive* • *HP DeskJet 340C Portable Printer* • *17" External Monitor* • *Xircom CardBus Ethernet II* • *Linux Software*	*1*	*$5,742*	*$5,742*
TOTAL			***$16,488***

Table 3 - Estimated Materials / Costs for Risk Analysis

Participant Roles

This project will be led by SEI, augmented as required by ATI, and ADL.

- **SEI** will lead the team in developing the methods, processes, tools, and training material as required for the risk assessments and in conducting the expert-led and self-directed risk assessments.
- **ATI** will provide support as required to the Risk Analysis team. This will include an ATI Senior Researcher experienced in the medical domain, in developing processes, and in training site staff will assist in identification and evaluation of vulnerabilities and risks, and in development and delivery of training if required. ATI technical staff will augment the team as required, drawing on their expertise to assist in identifying and evaluating risks and vulnerabilities and deriving subsequent recommendations for mitigation activities.
- **ADL** will provide support functions to the Risk Analysis effort that include: coordinating the availability and participation of the designated SEI, ATI, LMES, HOST, KRM, and MTF contributors; monitoring/reporting the Risk Analysis Team's against budget; coordinating availability of equipment/materials needed for Team use while onsite at the MTF; consolidation and publication of the Risk Analysis effort's Meeting Minutes and Trip Reports based on inputs provided by Risk Analysis Team members; collection/consolidation of captured Risk Analysis data, notes, and reports for turnover to TATRC's RIMR database; coordination and consolidation of required Risk Analysis documentation.

Long-Term Vision for Risk Analysis Work (DHIAP Phase III)

Transition SDRA from Pilot to Production Capability

DHIAP Phase III will focus on transitioning the Self-Directed Risk Assessment from a pilot to a production version able to be performed by additional MTFs. This will require the following:

- Refinement of the Self-Directed Risk Assessment and associated training – this task would refine the Self-Directed Risk Assessment method and training developed in DHIAP Phase II based on lessons learned from piloting them
- Train-the-trainer course – this task would develop and pilot a train-the-trainer course for the Self-Directed Risk Assessment method training

  The goal of this development effort would be to establish a path toward qualifying trainers to teach the Self-Directed Risk Assessment method.

Future R&D

Future areas of research and development in this area include:

- Developing a method for managing risk on a continual basis – this research area would examine ways in which organizations could manage their information security risks between deliveries of Risk Assessments
- Developing method for collaboratively managing risk among organizations – this research area would examine ways in which multiple organizations could work together to manage shared information security risks that arise from interdependencies in critical infrastructures

Both of the suggestions for future research areas listed above are major efforts that would be comparable in scope to the development of the Self-Directed Risk Assessment.

3. Business Case Analysis

The DHIAP Team will analyze the business conditions under which the US Army should deploy technologies for promoting health information assurance in its health care system. Included in the studies will be an assessment of feasibility, cost, benefit, and availability of information assurance technologies in access control, authentication, file integrity, and/or data transfer.

Lead Organization

Lockheed Martin Energy Systems (LMES)

Participants

ATI, KRM, HOST, ADL

Background

The DHIAP team will utilize proven methodology typically employed in business case analyses to perform this task. This methodology includes Metrics Definitions, Tangible and Intangible Benefits Identification, Data Collection and Analysis, and Results and Conclusions.

In the February 16-18 DHIAP Phase II Kickoff Meeting, it was agreed that the subjects to be studied in Business Case Analysis (BCA) should be re-evaluated. (A summary of changes is included in Table 4 below.) While BCAs should definitely incorporate investigation of feasibility, cost, benefit, and availability of specific technologies/combinations of technologies for access control, authentication, file integrity, and data transfer, the subjects addressed by BCAs should have a more direct relationship to the operational activities of MTFs and DoD. In addition, TATRC requested that the studies include the following perspectives where possible: Tri-Service including the VA, facility size/purpose (from outpatient clinic to regional medical center), and facility type (fixed, mobile, deployed). TATRC called for including the subject of network survivability in the studies where appropriate, and requested that the BCA Methodology and resulting data, reports, and potential technology demonstrations be constructed in a way that would permit their inclusion in TATRC's strategic Risk Information and Management Resource (RIMR).

Task 1 – Define Methodology

- Scope increase in the methodology/metrics effort as focused research on technology areas is replaced by the broader-scope investigation of MTF operational subjects and their use of technology
- New subtask to recommend candidate subjects for Business Case Analyses # 2-4

Task 2 – Conduct Studies/Produce Reports

- Designation of RADIUS as the first BCA study subject
- Reference to the investigation areas of BCAs # 2-4 as "to be determined"

Task 3 – Identify other candidate areas for BCAs

- Task deleted; Task 1 now covers this subject

Task 4 – Identify to TATRC Potential Technology Demonstrations

- Task deleted; subject covered as a subtask in each Task 2 BCA

Table 4 - Phase II Kickoff Meeting Changes to BCA Tasks

The BCA project's plans have been adjusted to fit with these requests. Major changes relative to earlier proposals are shown in Table 4 above. The descriptions of Major Activities in the next section reflect these changes.

Major Activities

3.1 Develop BCA Methodology/Metrics

The DHIAP Team will define a methodology and the metrics (including benefits and costs) that will determine the probable success of the given technology. The team will use methods most applicable to information assurance technology to determine the tangible benefits which include improvements in such things as cost reduction (purchase and sustainment), information access, and access control. They will also identify and measure the intangible benefits. While intangible benefits are real, they are not as easily measured as tangible benefits; they are generally defined as cost avoidance or risk mitigation factors. Intangible benefits that the DHIAP Team will observe include user satisfaction, fit with legacy systems, and customer support. The investigation will draw on team members' organizational and personal experience, will include literature research, and, when appropriate and approved by TATRC, will include hands-on investigation of representative products.

The DHIAP Team will incorporate the methodology and metrics described above into a formal process for conducting the Business Case Analyses. The process documentation will be drafted prior to performing the first Business Case Analysis, then refined prior to initiating the second one. The result will be a product suitable for use by the DHIAP Team in analyzing their information assurance needs and prioritizing their requirements. Use of the process should enable the MTF or MEDCOM decision-maker to narrow the broad range of technologies available down to those that benefit the MTF by addressing information assurance requirements as determined in DHIAP's Risk Analysis Project. The process will assist the MTF or MEDCOM decision-maker in further narrowing the candidate technologies by examining the business case of introducing each into the MTF information infrastructure.

Development of the Methodology/Metrics will include two team meetings to develop and refine the methodology. One of these meetings should include a visit to the Advanced Technology Integration Center (ATIC). Often team meetings for methodology development will be electronic.

3.2 Select BCA Subjects and Sites

The Kickoff Meeting called for a reassessment of the subjects to be addressed in the Business Case Analysis project. As is evident from the left-most list in Table 5, the subjects proposed for investigation are broad issues specific to technologies. Based on decisions made in the Kickoff, if one or more of these subject areas are germane to a BCA's focus, they will be included within the scope of this BCA investigation. The list on the right side of Table 5 summarizes the BCA subjects suggested during the meeting. The group agreed that selection of Phase II BCA focus areas be added to the scope of project effort, defined as a task that would be performed in about the same timeframe as the Methodology/Metrics definition effort. Additional information about selection plans is provided below.

Original BCA Subjects	Kickoff Meeting Candidate Subjects
1. Access Control	1. Remote Access Dial-In User System (RADIUS)
2. Authentication	2. Subjects Proposed in Earlier BCA Drafts:
3. File Integrity	▪ Security in Remote System Administration
4. Data Transfer	▪ Security Requirements to Support Staff Roles/Changes
	3. Subjects of Phase I Research Papers:
	▪ Remote System Administration
	▪ Public Key Infrastructure
	▪ Trust Model

Table 5 - Summary of Changes Proposed for BCA Investigations

Selection of BCA #1: It was agreed at the kickoff meeting that the initial Business Case Analysis would focus on the business case for remote dial-up. The subject was considered important to DoD and the Army; further, it seemed to be an appropriate first target because the DHIAP Team and two MTF demonstration sites have already developed extensive knowledge in this area during Phase I RADIUS (Remote Access Dial-In User System) development and demonstration efforts.

Selection of BCAs #2-4: The BCA Team will work with TATRC to develop recommendations for the subjects of BCAs #2-4. For each subject listed in Table 3, the team will prepare a summary of the appropriate BCA research and recommend characteristics of the sites and the scope of the investigation and analysis phases of the work. In addition, the team will provide their recommendation for the subjects to be selected for BCA. The team will present the BCA research summaries and their recommendations at the initial Interim Program Review (IPR) meeting for Phase II (tentatively scheduled for June 2000 at the SEI), then work closely with TATRC to select the subjects of BCAs #2-4 and refine plans as necessary. In the later Phase II IPRs, in addition to reporting status and results of active BCAs, the team will lead a reality check of plans for BCAs to be conducted in the remainder of Phase II and in Phase III.

Development of Business Case plans and recommendations will occur during the same timeframe and using the same resources as the Methodology/Metrics task.

3.3 Conduct BCAs

3.3.1 BCA #1: RADIUS (Remote Dial-Up Access)

3.3.1.1 Develop technical plan

The team will review the operational/functional requirement that necessitated the introduction of RADIUS technology and determine what operational, administrative, and technical questions should be asked to identify costs and benefits of RADIUS introduction. The team will then decide where and of whom to ask those questions.

The requirement to make the analyses relevant to all services and facilities will add complexity to the questions and the sources of answers.

3.3.1.2 Perform analysis

The team will collect the information identified in the plan. In many cases, the collecting will generate new questions and new places to ask questions. After collecting information, the team will categorize data into technical, operational, and administrative costs and benefits. Other categories may arise. Relevance of costs and benefits may not be readily apparent or consistent across the services. Sources of further information on the specific products related to a given technical case will be identified.

3.3.1.3 Identify tech demo (if appropriate)

Identify to TATRC any potential technology demonstrations appropriate to determine effectiveness and feasibility of adapting the technology into MTFs or the Resource Information Management Resource (RIMR). Before any acquisition, each demonstration candidate will be discussed with the DHIAP COR and COR's technical staff, with the team outlining the relevance of the proposed demonstration and recommending the site(s) most appropriate for conducting the demonstration. When appropriate, the ATIC, the distributed DHIAP laboratory, and/or RIMR will be used for demos. Resource estimates for this step will be determined if and when appropriate.

3.3.1.4 Develop/publish Final Report

The team will present the costs and benefits in a manner meaningful to MTF commanders and Information Management Officers. Conclusions will be presented with appropriate caveats. The report will be delivered in a format suitable for RIMR.

3.3.1.5 Update Final Report based on demo (if appropriate)

The team will modify the final report as needed based on results of the demonstration.

3.3.2 BCA #2

- Develop technical plan - *These steps will be similar for each case.*
- Perform analysis
- Identify tech demo (if appropriate)
- Develop/publish Final Report
- Update Final Report based on demo (if appropriate)

3.3.3 BCA #3

- Develop technical plan - *These steps will be similar for each case. By this time, there will probably be sufficient progress in the Risk Assessment Project that some input can be collected from participating in that activity.*
- Perform analysis
- Identify tech demo (if appropriate)

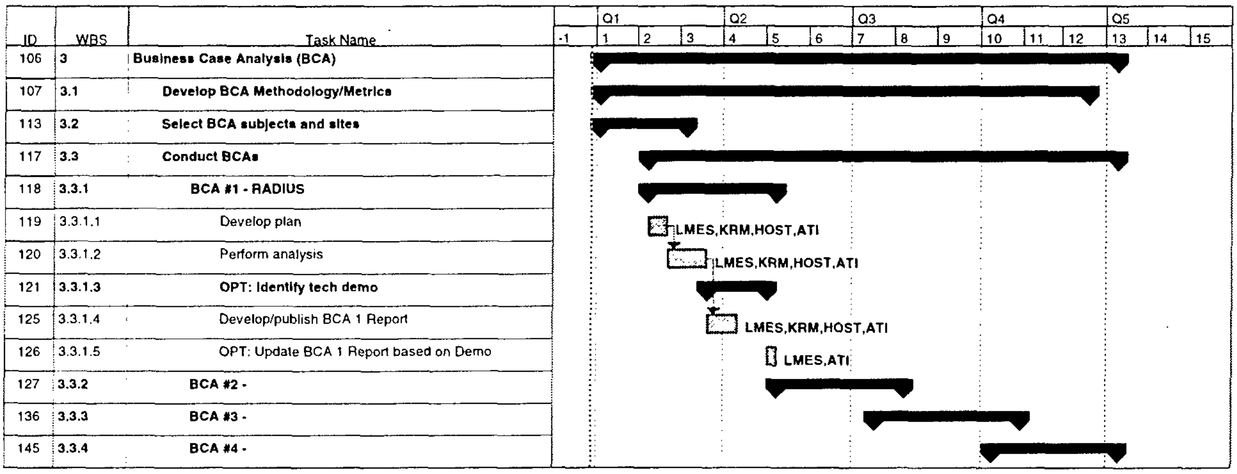
- Develop/publish Final Report
- Update Final Report based on demo (if appropriate)

3.3.4 BCA #4

- Develop technical plan - *These steps will be similar for each case.*
- Perform analysis
- Identify tech demo (if appropriate)
- Develop/publish Final Report
- Update Final Report based on demo (if appropriate)

Schedule

Figure 3 indicates the activities, planned timeframes, and participants of the major activities of the Business Case Analysis effort.



ID	WBS	Task Name
106	3	**Business Case Analysis (BCA)**
107	3.1	**Develop BCA Methodology/Metrics**
113	3.2	**Select BCA subjects and sites**
117	3.3	**Conduct BCAs**
118	3.3.1	**BCA #1 - RADIUS**
119	3.3.1.1	Develop plan
120	3.3.1.2	Perform analysis
121	3.3.1.3	**OPT: Identify tech demo**
125	3.3.1.4	Develop/publish BCA 1 Report
126	3.3.1.5	OPT: Update BCA 1 Report based on Demo
127	3.3.2	**BCA #2 -**
136	3.3.3	**BCA #3 -**
145	3.3.4	**BCA #4 -**

Figure 3 - WBS Gantt Chart for Business Case Analysis

Issues/Dependencies

- Designation of subjects to be addressed by BCAs: TATRC will select subjects to be investigated based on input provided by this project's first step, "Determination of Analyses to be Performed in the Business Case Analysis Project."
- Engagement of BCA sites: The government will identify sites willing to participate in the business case analyses. The DHIAP Team will be prepared to brief command and MTF leaders regarding the BCA process and their participation.
- Lead time to assure team member availability: The DHIAP Team must know the BCA investigation subjects in order to reserve availability of staff who have appropriate expertise.
- DoD subscription: TATRC will investigate the availability of the Gartner Group and the IATAC subscriptions as Government Funded Equipment resources to help supplement the BCAs, thereby saving some time and expense of DHIAP-led detailed technology evaluations.

- Technology demonstrations relating to Business Case Analyses: Candidate technologies for demonstration will be presented for discussion and approved by the DHIAP COR prior to commencement of demonstration development.
- Information sharing with the Risk Analysis Team: The Business Case Analysis team will provide the draft Business Case Analysis Methodology to the Risk Assessment team to influence the type of information collected during Risk Assessments. In return, information collected during Risk Assessments will, when available and relevant, be incorporated into Business Case Analyses.
- Identification of other Business Case Analysis work being performed in the military: TATRC will monitor other BCA work being performed in the military to assure that DHIAP efforts do not address the same or similar areas.

Deliverables

1. Description of the methodology and metrics for Business Case Analysis applied to information assurance technology (electronic and hard copy)
2. White papers on the Business Case Analyses performed during the project, including a summary of technology demonstrations if authorized by TATRC (electronic and hard copy)
3. As appropriate, proposals for BCA-related technology demonstrations recommended to determine the effectiveness and feasibility of adaptation of technologies into MTF.
4. All reports and raw data resulting from Task 3 in electronic format suitable for inclusion in RIMR. (Reports will be provided to TATRC in MS Word format, and all raw data collected during the course of work groups and interview sessions will be provided using generally available, affordable tools such as MS Access, Excel, or Word as appropriate to the type of information collected. The initial project task for "development of the methodology" will include definition of the data to be collected and the tools to be used in recording it for RIMR.)

Travel

The work of this project will rely on expert knowledge augmented by literature search and will build on experience gained in Information Security Evaluations, Risk Analyses, and previous BCAs. In general travel will be required to develop the Methodology and then to coordinate directly with MTF sites to assess/understand existing conditions and the suitability of potential improvements, install/implement demonstrations at ATIC/RIMR, MTF sites and/or the distributed DHIAP laboratory, and understand operational impact. The sites for Phase II BCAs have not been selected as of yet. For costing purposes we have assumed that the sites participating in Phase I demonstrations would be good candidates for the first BCA, RADIUS. For BCAs # 2-4, we identified other locations that each offer the potential for working with MTFs of two or more military services. Table 6 below provides additional information about the participating organizations and number of travelers for each event. Note that the Team Members column indicates "(TATRC)" for trips involving subjects that the TATRC team members may wish to participate in. This information is provided for TATRC's budgeting of potential travel.

Month	To	Reason	Team Member(s)	Contractor Travelers
Awd + 1	Charleston, SC	Develop Initial Methods/Metrics	ATI, LMES, HOST, KRM	4
Awd + 2	Washington, DC	Develop Plan for RADIUS BCA, Visit ATIC	ATI, LMES, KRM, HOST, (TATRC)	6
Awd + 2	Augusta, GA and Savannah, GA	Perform RADIUS BCA Analysis	ATI, LMES, KRM, HOST, (TATRC)	6
Awd + 5	Charleston, SC	Refine Methodology; Plan BCA #2	ATI, LMES, KRM, HOST	3
Awd + 6	Norfolk, VA	Perform Analysis on BCA #2; Plan BCA #3	ATI, LMES, KRM, HOST	5
Awd + 8	San Antonio, TX	BCA #3: Analysis	ATI, LMES, HOST, (TATRC)	3
Awd + 10	Teleconference (no travel)	BCA #4: Plan	ATI, LMES, HOST	0
Awd + 11	Washington, DC	BCA #4: Analysis	ATI, LMES, HOST, (TATRC)	3

Table 6 - Projected Travel for Business Case Analysis

Equipment

As determined in the Kickoff Meeting, the team plans to utilize access to a DoD subscription with a resource that performs technology evaluations on a routine basis or on request (sources of this information include Gartner Group and IATAC). TATRC has agreed to investigate availability of these resources as Government Funded Equipment and to try to make them available to support and supplement the BCAs, thereby saving some time and expense of DHIAP-led detailed technology evaluations.

Some equipment acquisition is proposed with the BCA project to give the DHIAP program the flexibility to test and demonstrate emerging technology in order to validate the application of the technology to the healthcare domain. Some candidates for technical demonstrations include the following:

- Authentication server and client software system to support strong user authentication
- Proxy server system to provide Web, Telnet and FTP filtering and control
- Public key infrastructure (PKI) client and certificate software systems to explore potential extension applicable to healthcare such as attribute certificates and non-repudiation
- Combining a secure web interface with a terminal session

Support for these demonstrations may require platforms capable of emulating characteristics of any current operating system. For costing equipment for this proposal, the team limited the proposed environment to Windows NT and Linux clients, although other devices may be necessary to fully support technology demonstrations. We predict that, as we use the RADIUS

NT server to support enhancement of server software, an upgrade to the server capability may also be necessary.

As stated in BCA activity descriptions, each candidate for demonstration will be closely coordinated with the DHIAP COR and the COR's technical staff prior to submitting a request to Army Contracts for equipment acquisition. Discussions will outline the relevance of the proposed demonstration and suggest the site(s) where demonstration would be most appropriate. Candidate sites for conducting the demonstrations include TATRC, MTFs, ATI, LMES, and ATIC. The demonstrations would be relevant to TATRC, MTFs, MEDCOM, and DoD depending on technology and technical approach being demonstrated. Table 7 provides a high-level cost estimate of materials appropriate for conducting candidate demonstrations. The actual types and costs of equipment will be highly dependent on the focus of BCAs that are selected by DHIAP COR and the COR's technical staff.

Description	Cost
Authentication server and client software systems	$17,000
Proxy server software	$3,000
PKI client and certificate software and license	$1,350
Client computers (NT and Linux)	$10,700
Misc items including server and client hardware and software upgrades	$6,585
TOTAL	**$38,635**

Table 7 - Estimated Materials / Costs for Potential Demonstrations

Participant Roles

This project will be led by LMES, augmented as required by ATI, KRM Associates, HOST, and ADL.

- **LMES** will lead the team in conducting studies of feasibility, cost, benefit, and availability of select information assurance technologies. LMES will collaborate with ATI for development, implementation, and demonstration of any technologies approved to support the analyses.
- **ATI** will provide the DHIAP PI as required to support collaborative work with LMES on approved technology demonstrations. ATI will also provide a Senior Researcher who has extensive experience in healthcare operations and healthcare's use of information technology. ATI's PI, Senior Researcher, and Researcher have extensive experience with the RADIUS technology implementations at the Phase I testbed sites as well as with the MTF staff involved in the effort. Use of this operational experience (as a complement to LMES' design-oriented experience with the technology) is the most efficient and cost-effective way to accomplish technology- and site-specific tasks determined to be part of the Business Case Analysis methodology (to be defined). In addition, the technical skills of the ATI Senior Researcher, Systems Analyst, and Researcher will be applied in one or more of the other three BCAs planned for this task and to any technology demonstrations approved for the four BCAs.

- **KRM Associates** will provide an expert well versed in performing Business Case Analyses to participate in conducting analyses and provide expert guidance, review, and advice on the business case analysis process. The consultant's contributions will focus on methodology and business processes, while other members of the team are contributing the technical expertise and experience.
- **HOST** (Healthcare Open Systems & Trials consortium) will provide its Executive Director, a consultant with extensive experience in the military medical domain, to participate in the analyses and provide expert guidance, review, and advice on military healthcare aspects of the business case analyses. The consultant's contributions will focus on the military healthcare system, while the other members of the team contribute technical expertise and experience.
- **ADL** will provide financial expertise to LMES in the feasibility and cost/benefit analyses associated with the business case analyses. ADL will also provide material management and control support during the material procurement required in the implementation and demonstration phase of this project.

Long-Term Vision for Business Case Analysis Work (DHIAP Phase III)

MTF Self-Performed Business Case Analysis

The MTFs and their parent command will be making technology selections indefinitely. Legislation and information assurance threats will demand different forms of information and system protection, and the evolution of standard and local information systems will necessitate re-evaluation of the protective measures on those systems. Hence, the need to evaluate information assurance technologies on their technical, business, economic, and administrative merits will not go away.

The team proposes to investigate the development of a business case analysis methodology that can be applied by the MTF command, IMD, and other appropriate staff. The experience that will be gained during this task in DHIAP Phase II should provide sufficient understanding of the diverse technical, operational, economic, and administrative factors affecting fixed and deployed MTFs of all sizes and all services. DHIAP Phase III deliverables to support MTFs include:

- A business case methodology suitable for execution by the MTFs
- Demonstrations of MTF-level self-performed Business Case Analysis

Tri-Service Applicability of Business Case Analyses

While effort will be made during Phase II to include considerations of all military services in the findings of DHIAP Business Case Analyses, budget and time constraints preclude assuring that all significant cross-service differences were accounted for. In Phase III, the DHIAP Team will extend investigation into military services in addition to the Army to assure that the conclusions and recommendations of Phase II BCAs are described in terms appropriate to each of the services and that recommendations for future BCAs incorporate issues and concerns of each of the services.

4. Simulation Capability

The DHIAP Team will create the technical and organizational capability to run simulations for mission survivability of defense healthcare infrastructure.

Lead Organization

Software Engineering Institute (SEI)

Participant

ATI

Background

The objective of this effort is to design and implement an automated simulation system that can be used to demonstrate, validate, and depict problems and solutions in mission survivability for Army medical systems.

The survivability simulation system is part of a long-term research and development effort to better understand and develop more effective methods for addressing security and survivability issues in networked systems, with particular emphasis on critical national infrastructures including military healthcare infrastructure. Survivability is the ability of a system to continue to fulfill the most critical aspects of its mission under adverse conditions, whether those conditions are intrusions by electronic means, design errors in COTS software, accidents, corrupted data, or user errors.

A survivability simulation system will permit stakeholders to better understand the risks and consequences of cyber-based attacks on medical information systems. It could help uncover threats and improve protection of integrity, confidentiality and availability of patient records, treatment plans, and essential medical services. The simulation system and closely related work in survivability research should lead to improved management decisions and cost-effective tradeoffs for protecting medical information systems and should also enable "what if" analyses, contingency and disaster planning, and recovery. The survivability simulation system could serve as a mechanism for analyses and validation of proposed changes and improvements to existing medical information infrastructure.

Major Activities

4.1 Develop/demonstrate Survivability Simulator

The technical approach to the simulation development includes (1) design of a discrete event simulation programming language, (2) implementation of a translator, a run-time system, and a visualization system for that language, and (3) development of documentation for simulation authors and users. The survivability simulation system is being developed under the direction of Dr. David A. Fisher at the SEI. The CY2000 work on the survivability simulation system will be focused on the implementation effort. The preliminary functional version (i.e., alpha release) of the survivability simulation system will be completed during the period of performance. The alpha version will enable test use of the survivability simulation system within the SEI facility. The survivability simulator will be implemented on a widely available uniprocessor system using a generic form of C code to minimize the effort to port the system to multiple platforms. The first priority, however, is to obtain a fully functional version that can be used to test and demonstrate the capabilities of the system, to validate design decisions, and to conduct research in survivability that is infeasible without a simulator. This task also includes design and implementation of both unit and integration tests on an ongoing basis throughout the implementation.

4.2 Provide Preliminary Manual and Guide

Easel Language Reference Manual (ELRM)

Easel Author Style Guide (EASG)

The simulation language, called "Easel," is a high level programming language with specialized features for abstract specification of mission requirements and constraints; for simulation of distributed systems including concurrent execution, communication without shared memory, physical position and locality control, and intruder actions; and for dynamic depiction of a simulation from multiple perspectives. Documentation for the system will focus on its use in depicting, understanding, and analyzing a system's survivability and security through simulation and from the perspective of mission-oriented risk management. During the period of performance, a preliminary version of the Easel Language Reference Manual (ELRM) and the Easel Author Style Guide (EASG) will be released.

4.3 Coordinate with Advisory Groups and Conduct Technical Meetings

The simulation capability effort will work with TATRC, an Army Simulation Advisory Group to be identified by TATRC, and Subject Matter Experts (SMEs) to develop a plan for use of the simulation system in Army medical systems. This task includes related research on effective use of the simulation system in survivability of Army, medical, and related infrastructural applications. A minimum of four technical meetings at Army or SME sites is required for this task.

It is anticipated that one or more Carnegie Mellon University (CMU) graduate students will do project-related MS theses, depending on the level of interest from students. These students will conduct related research at regional medical centers or other appropriate locations on the effective use of the simulation system in survivability of Army, medical, and related infrastructural applications.

4.4 Develop and Demonstrate Simulation Capability

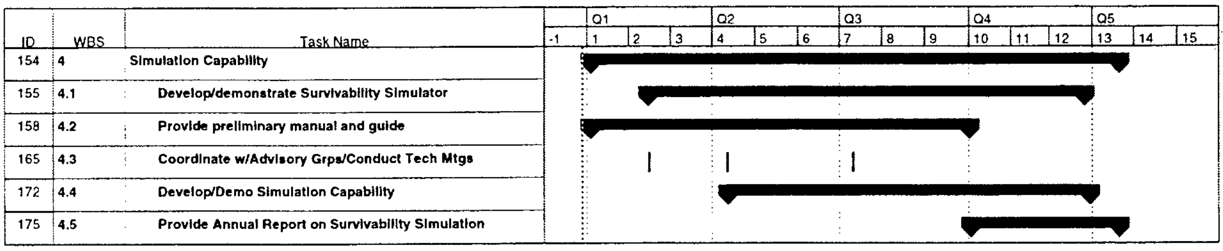
The Simulation Capability demonstration will include key features of the survivability simulation system from author and user perspectives. The demonstration will include a review of the goals and purpose, live program executions, and anticipated benefits in survivability of Army medical systems. The demonstration will be given to TATRC at Ft. Detrick approximately 30 days after the alpha release of the survivability simulation system.

4.5 Provide Annual Report on Survivability Simulation

The annual report of the Simulation Capability effort will include progress to date on the design and implementation of the simulation language and system and on related research. It will include the ELRM, the EASG, and any research papers presented at professional conferences and workshops or published in other forms.

Schedule

Figure 4 below indicates the activities, planned timeframes, and participants of the major activities of the Simulation Capability project.



ID	WBS	Task Name
154	4	Simulation Capability
155	4.1	Develop/demonstrate Survivability Simulator
158	4.2	Provide preliminary manual and guide
165	4.3	Coordinate w/Advisory Grps/Conduct Tech Mtgs
172	4.4	Develop/Demo Simulation Capability
175	4.5	Provide Annual Report on Survivability Simulation

Figure 4 - WBS Gantt Chart for Simulation Capability

Issues/Dependencies

- Availability of Simulation Advisory Group (SAG) members and Subject Matter Experts (SMEs): TATRC will identify SAG and SME members with appropriate expertise to offer insight into the survivability requirements, knowledge of Army medical infrastructure, and where simulation could be most beneficial to the Army.
- Availability of TATRC representative for onsite training/participation at SEI: TATRC will identify candidates who could be resident at the SEI for 6 to 12 months, beginning September 2000 or later, to participate directly in the survivability simulation effort and gain hands-on experience that can be transitioned back to the Army.
- Availability of graduate students to perform project-related research: SEI will identify CMU graduate students conducting project-related research in survivability of Army, medical, and related infrastructural applications.

Deliverables

1. Preliminary functional version (i.e., alpha release) of the survivability simulation system
2. Preliminary version of the Easel Language Reference Manual (ELRM) detailing the syntax, semantics, and all built-in types and operations of the language
3. Preliminary version of the Easel Author Style Guide (EASG) providing examples and discussion of how Easel can and is intended to be used to address a variety of simulation problems
4. Meetings with TATRC, Army Simulation Advisory Group, and Subject Matter Experts on plans for Army use of the survivability simulation system
5. Functional demonstration of the simulation capability at Ft. Detrick
6. Annual Report of Survivability Simulation

Travel

The work of this project will be based at the SEI in Pittsburgh PA. Travel will be required for meetings with TATRC, the SAG, and the SMEs. For estimating purposes, these meetings were defined as occurring in Ft. Detrick MD, Washington DC, San Antonio TX, and an Army Simulation Facility in Orlando, FL. The DHIAP PI will attend and coordinate these meetings.

In addition, there will be some travel for CMU graduate-level students conducting related research on the effective use of the simulation systems in survivability of Army, medical, and related infrastructural applications. While these individuals will visit locations determined at the time to be most appropriate for estimating purposes the following locations were assumed: San Diego CA, San Antonio TX, and Washington DC. There will also be some travel and attendance at two of the several technical conferences where which papers related to this effort will be presented: Network and Distributed System Security Symposium in San Diego CA and the Information Survivability Workshop (ISW '00) in Boston MA.

Table 8 below provides additional information about the participating organizations and number of travelers for each event. Note that the Team Members column indicates "(TATRC)" for trips involving subjects that the TATRC team members may wish to participate in. This information is provided for TATRC's budgeting of potential travel.

Month	To	Reason	Team Member(s)	Contractor Travelers
Awd + 1	Ft. Detrick, MD	Technical Meetings / Briefings	ATI, SEI, (TATRC)	3
Awd + 2	San Diego, CA	Medical Fact Finding	SEI	1
Jun-00	San Diego, CA	Conference	SEI	1
Awd + 4	Washington, DC	Technical Meetings / Briefings	ATI, SEI, (TATRC)	3
Awd + 4	San Antonio, TX	Medical Fact Finding	SEI	1
Sep-00	Boston, MA	Conference	SEI	1
Awd + 7	San Antonio, TX	Technical Meetings / Briefings	ATI, SEI, (TATRC)	3
Awd + 7	Washington, DC	Medical Fact Finding	SEI	1
Awd + 10	Orlando, FL	Technical Meetings / Briefings	ATI, SEI, (TATRC)	3

Table 8 - Projected Travel for Simulation Capability

Equipment

Any equipment required for the Simulation Capability project will be funded through non-DHIAP sources.

Participant Roles

This project will be led by the SEI, augmented as required by ATI.

- **SEI** will lead the team in designing and implementing an automated simulation system that can be used to demonstrate, validate and depict problems and solutions in mission survivability for Army medical systems.

- **ATI** will provide the DHIAP PI to facilitate SEI's cooperation with the senior leadership within the Military Medical Commands and in developing long-term plans. ATI will also provide a Senior Researcher with extensive medical domain knowledge and experience to provide operational advice as appropriate.

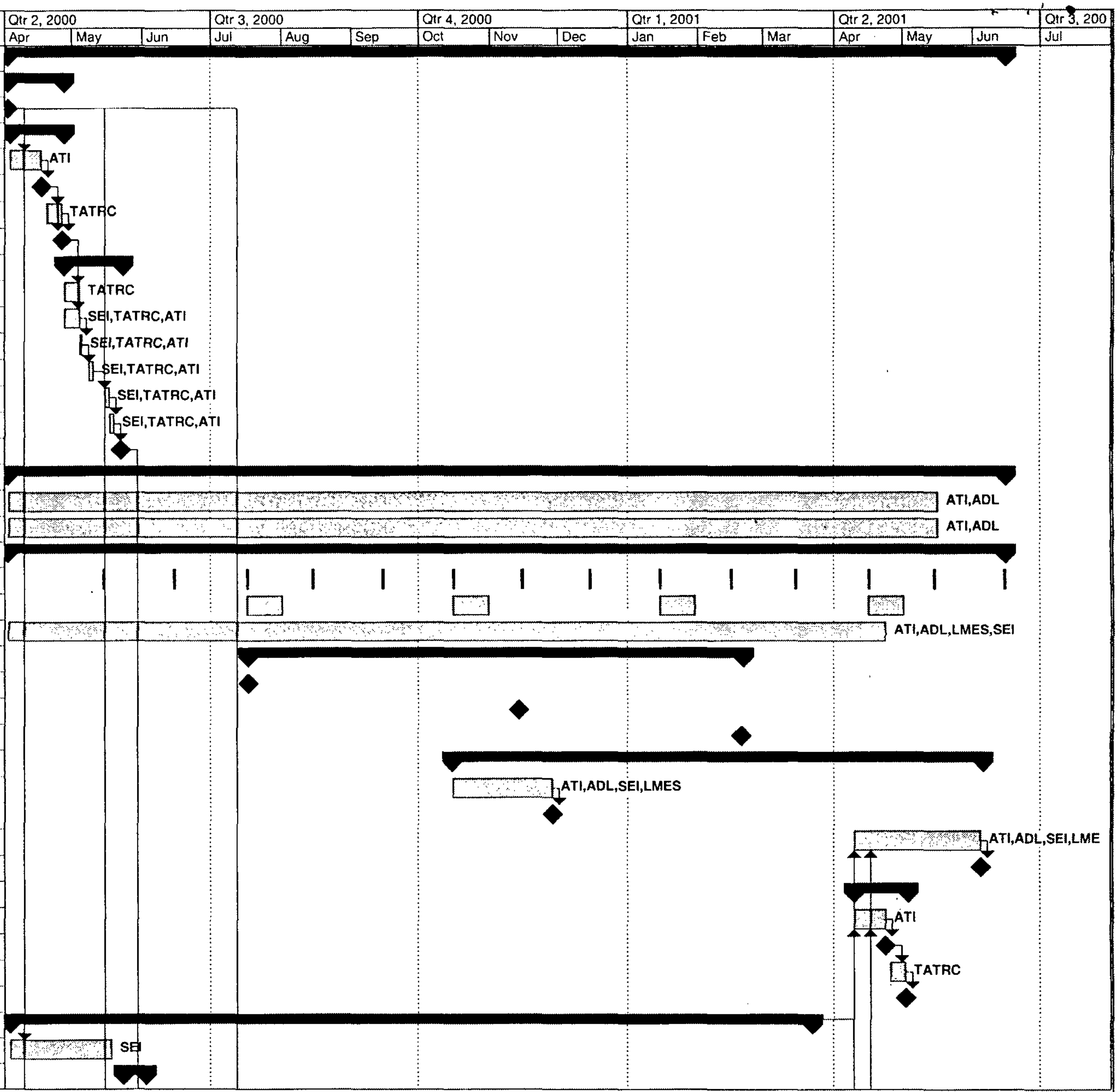
Long-Term Vision for Simulation Capability Work (DHIAP Phase III)

The long-term purpose of the Simulation Capability is to develop effective solutions to security and mission survivability problems that exceed the inherent limitations of existing security technologies. The simulator will provide greater insight into the character of these problems for researchers, practitioners, and executive decision makers. It will help all three classes of stakeholders to better understand the risks that they must manage and their potential consequences. The simulator will also serve as a tool for research in finding new solutions to security, survivability, and infrastructure assurance problems. It should be especially helpful where solutions are required that involve technical advances in unbounded systems, emergent algorithms, survivability architectures, dynamic trust, or validation of critical mission requirements. The following items are appropriate next step tasks once the alpha version of the simulator is available:

- Beta version of the Survivability Simulator
- SEI Resident Affiliate from Army medical applications
- Continued research in Army medical infrastructure requirements
- Continued research in Army medical infrastructure solutions
  - Web-enabled version of the Survivability Simulator
  - Training course in the use of the Survivability Simulator
  - Develop library of reusable components specialized for Army and medical infrastructure applications
  - Develop an automated interface to existing Army database for easier access to realistic simulation parameters

THIS PAGE INTENTIONALLY LEFT BLANK

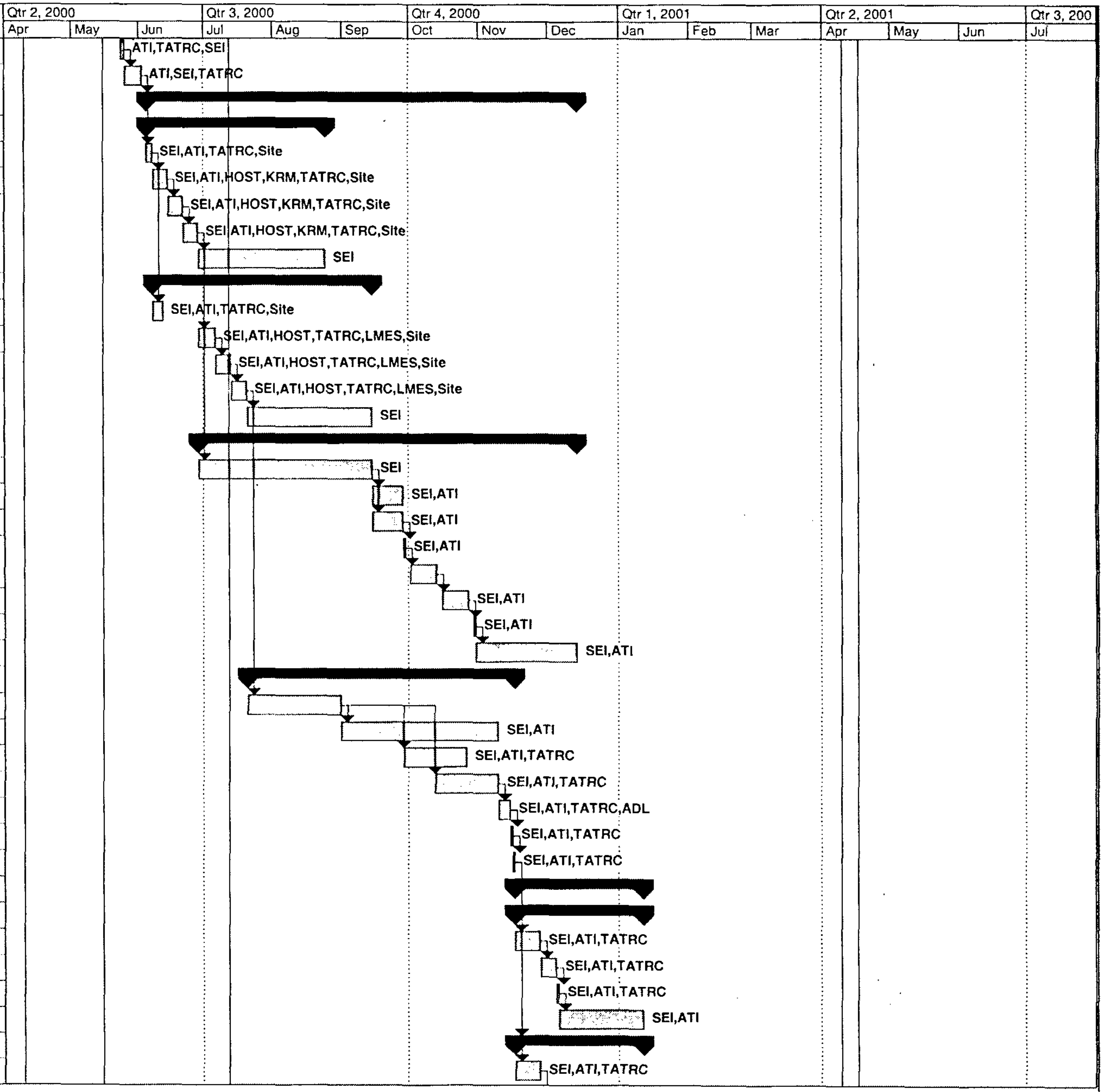
ID	WBS	Task Name
1	1	**Program Management**
2	1.1	**Initiate Phase II Work**
3	1.1.1.6	Approve Tech Devel Plan
4	1.1.2	**Initial Command Briefing**
5	1.1.2.1	Develop briefing
6	1.1.2.2	Draft briefing to TATRC
7	1.1.2.3	Schedule initial command briefing
8	1.1.2.4	Present initial command briefing
9	1.2	**Recruit Sites**
10	1.2.1	Identify candidate sites
11	1.2.2	Prepare site-level briefing
12	1.2.3	*Present to DDEAMC (Augusta) & WACH (Savannah)*
13	1.2.4	Present to Ft. Eustiss & Ft. Bragg
14	1.2.5	Present to San Antonio & Seattle
15	1.2.6	Recommend sites to TATRC
16	1.2.7	Designate selected sites
17	1.3	**Manage DHIAP Activities**
18	1.3.1	Manage DHIAP technical work
19	1.3.2	Facilitate project and cross-project activities
20	1.3.3	**Provide regular project reporting**
21	1.3.3.1	**Develop Monthly Reports**
36	1.3.3.2	**Develop Quarterly Reports**
41	1.3.3.3	*Provide Meeting Minutes and Trip Reports*
42	1.4	**Conduct Team IPRs/Command Briefings**
43	1.4.1	IPR #1: Pittsburgh, PA
44	1.4.2	IPR #2: VTC / Teleconference
45	1.4.3	IPR #3: Charleston, SC
46	1.5	**Provide Annual/Final Reports**
47	1.5.1	Develop Annual Report
48	1.5.2	Deliver Annual Report
49	1.5.3	Develop Final Report (if rqd)
50	1.5.4	Deliver Final Report (if rqd)
51	1.6	**Summary Command Briefing**
52	1.6.1	*Develop briefing*
53	1.6.2	Draft briefing to TATRC
54	1.6.3	Schedule final command briefing
55	1.6.4	Present final command briefing
56	2	**Risk Assessment (RA)**
57	2.1	Design/develop OCTAVE tools & methodology
58	2.2	**Recruit/Select Sites for OCTAVE-based RA**



Project: DHIAP Phase II
Date: Mon 10/22/01
1:58 PM

Task	▨	Summary	▬	Rolled Up Progress	▬	Project Summary	▨
Progress	▬	Rolled Up Task	▨	Split	⋯	External Milestone	◇
Milestone	◆	Rolled Up Milestone	◇	External Tasks	□	Deadline	⇩

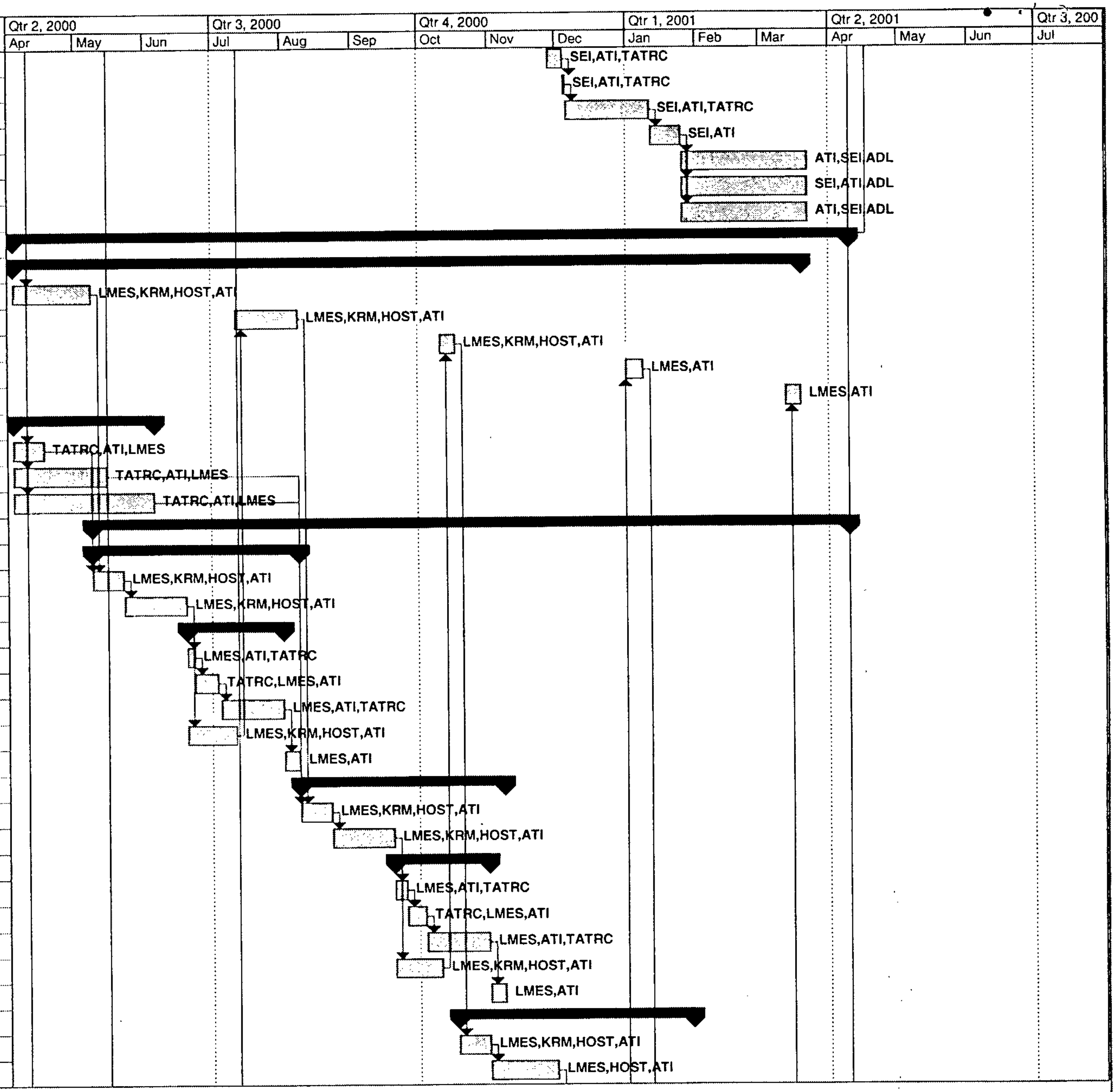
ID	WBS	Task Name
59	2.2.1	Notify sites of selection for OCTAVE
60	2.2.2	Schedule site engagements
61	**2.3**	**Conduct DHIAP-led RAs atTwo MTFs**
62	**2.3.1**	**Perform Site 1 OCTAVE I/II**
63	2.3.1.1	Provide preliminary briefing, plan w/site staff
64	2.3.1.2	OCTAVE I/II assessments
65	2.3.1.3	Analyze data/refine
66	2.3.1.4	Follow-on OCTAVE I/II assessments
67	2.3.1.5	Document baseline
68	**2.3.2**	***Perform Site 2 OCTAVE Phase I/II***
69	2.3.2.1	Provide preliminary briefing, plan w/site staff
70	2.3.2.2	Preliminary OCTAVE I/II assessments
71	2.3.2.3	Analyze data/refine
72	2.3.2.4	Follow-on OCTAVE I/II assessments
73	2.3.2.5	Document baseline
74	**2.3.3**	**Design/Perform OCTAVE III, sites 1-2**
75	2.3.3.1	Complete OCTAVE III design
76	2.3.3.2	Perform Site 1 OCTAVE III anal/assess
77	2.3.3.3	Analyze Site 1 results
78	2.3.3.4	Site 1 Exit Briefing
79	2.3.3.5	Site 2 OCTAVE III analysis/assessment
80	2.3.3.6	Analyze Site 2 results
81	2.3.3.7	Site 2 Exit Briefing
82	2.3.3.8	Provide Site 1-2 data/reports to TATRC
33	**2.4**	**Develop/Deliver SDRA training**
84	2.4.1	Refine Methodology
85	2.4.2	Develop SDRA training
86	2.4.3	Schedule SDRA training for Sites 3-4
87	2.4.4	*Schedule SDRA's for Sites 3 & 4*
88	2.4.5	Conduct SDRA Training for Sites 3-4
89	2.4.6	Conduct pre-assessment visit to Site 3
90	2.4.7	Conduct pre-assessment visit to Site 4
91	**2.5**	**Mentor SDRAs at Two MTFs**
92	**2.5.1**	**Conduct SDRA at Site 3**
93	2.5.1.1	Guide/mentor MTF staff during SDRA
94	2.5.1.2	Support site's analysis/prep of Exit Briefing
95	2.5.1.3	Support site's Exit Briefing
96	2.5.1.4	Site data/reports to TATRC
97	**2.5.2**	**Conduct SDRA at Site 4**
98	2.5.2.1	Guide/mentor MTF staff during SDRA



Project: DHIAP Phase II
Date: Mon 10/22/01
1:58 PM

Task	▨	Summary	▬	Rolled Up Progress	▬	Project Summary	▨
Progress	▬	Rolled Up Task	▨	Split	....	External Milestone	◇
Milestone	◆	Rolled Up Milestone	◇	External Tasks	□	Deadline	⇩

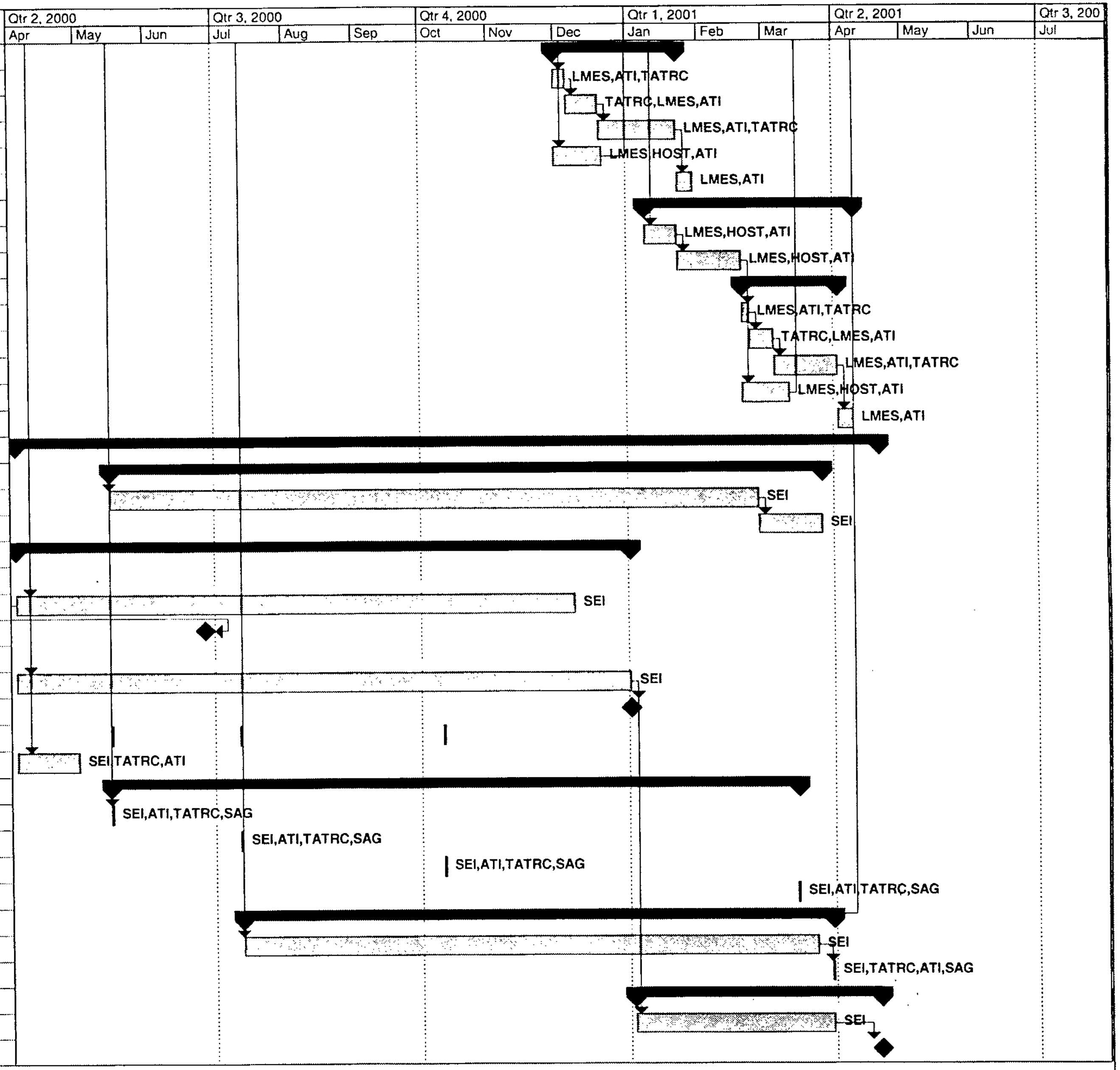
ID	WBS	Task Name
99	2.5.2.2	Support site's analysis/prep of Exit Briefing
100	2.5.2.3	Support site's Exit Briefing
101	2.5.2.4	Site data/reports to TATRC
102	2.6	SDRA method/training/templates/checklists to RIMR
103	2.7	Prepare RA Composite Report
104	2.8	Prepare Assessment State-of-the Practice Report
105	2.9	Prepare Change Report on differences at Phase I & II Sites
106	**3**	**Business Case Analysis (BCA)**
107	**3.1**	**Develop BCA Methodology/Metrics**
108	3.1.1	Develop initial methods/metrics
109	3.1.2	Refine/Publish Methodology
110	3.1.3	Refine Methodology re:BCA #2
111	3.1.4	Refine Methodology re:BCA #3
112	3.1.5	Refine Methodology re:BCA #4
113	**3.2**	**Select BCA subjects and sites**
114	3.2.1	Recruit sites for BCA#1(RADIUS)
115	3.2.2	Select subjects/sites of BCAs #2-4
116	3.2.3	Recruit sites for BCAs #2-4
117	**3.3**	**Conduct BCAs**
118	**3.3.1**	**BCA #1 - RADIUS**
119	3.3.1.1	Develop plan
120	3.3.1.2	Perform analysis
121	**3.3.1.3**	**OPT: Identify tech demo**
122	3.3.1.3.	Select techs to be demo'd
123	3.3.1.3.:	Coordinate w/demo site
124	3.3.1.3.:	Conduct demo
125	3.3.1.4	Develop/publish BCA 1 Report
126	3.3.1.5	OPT: Update BCA 1 Report based on Demo
127	**3.3.2**	**BCA #2 -**
128	3.3.2.1	Develop plan
129	3.3.2.2	Perform analysis
130	**3.3.2.3**	**OPT: Identify tech demo**
131	3.3.2.3.	Select techs to be demo'd
132	3.3.2.3.:	Coordinate w/demo site
133	3.3.2.3.:	Conduct demo
134	3.3.2.4	Develop/publish BCA 2 Report
135	3.3.2.5	OPT: Update BCA 2 Report based on Demo
136	**3.3.3**	**BCA #3 -**
137	3.3.3.1	Develop plan
138	3.3.3.2	Perform analysis



Project: DHIAP Phase II
Date: Mon 10/22/01
1:58 PM

Task	▨	Summary	■	Rolled Up Progress	■	Project Summary	▨
Progress	■	Rolled Up Task	▨	Split	....	External Milestone	
Milestone		Rolled Up Milestone		External Tasks	▭	Deadline	

ID	WBS	Task Name
139	**3.3.3.3**	**OPT: Identify tech demo**
140	3.3.3 3.	Select techs to be demo'd
141	3.3.3.3.:	Coordinate w/demo site
142	3.3.3.3.:	Conduct demo
143	3.3.3.4	Develop/publish BCA 3 Report
144	3.3.3.5	OPT: Update BCA 3 Report based on Demo
145	**3.3.4**	**BCA #4 -**
146	3.3.4.1	Develop plan
147	3.3.4.2	Perform analysis
148	**3.3.4.3**	**OPT: Identify tech demo**
149	3.3.4.3.	Select techs to be demo'd
150	3.3.4.3.:	Coordinate w/demo site
151	3.3.4.3.:	Conduct demo
152	3.3.4.4	Develop/publish BCA 4 Report
153	3.3.4.5	OPT: Update BCA 4 Report based on Demo
154	**4**	**Simulation Capability**
155	**4.1**	**Develop/demonstrate Survivability Simulator**
156	4.1.1	Develop alpha version simulator
157	4.1.2	Demonstrate alpha Survivability Simulator at SEI
158	**4.2**	**Provide preliminary manual and guide**
159	**4.2.1**	**Develop Easel Language Ref Manual (ELRM)**
160	4.2.1.1	Develop preliminary version of ELRM
161	4.2.1.2	Deliver preliminary version of ELRM
162	**4.2.2**	**Develop Easel Author Style Guide (EASG)**
163	4.2.2.1	Develop preliminary version of EASG
164	4.2.2.2	Deliver preliminary version of EASG
165	**4.3**	**Coordinate w/Advisory Grps/Conduct Tech Mtgs**
166	4.3.1	Identify/enroll Simulation Advisory Group
167	**4.3.2**	**Conduct Technical Meetings/Briefings**
168	4.3.2.1	Conduct Technical Meeting
169	4.3.2.2	Conduct Technical Meeting
170	4.3.2.3	Conduct Technical Meeting
171	4.3.2.4	Conduct Technical Meeting
172	**4.4**	**Develop/Demo Simulation Capability**
173	4.4.1	Develop demonstration
174	4.4.2	Present demonstration
175	**4.5**	**Provide Annual Report on Survivability Simulation**
176	4.5.1	Develop Annual Report
177	4.5.2	Deliver Annual Report



Project: DHIAP Phase II
Date: Mon 10/22/01
1:58 PM

Task	▨	Summary	■	Rolled Up Progress	■	Project Summary	▨
Progress	■	Rolled Up Task	▨	Split	··············	External Milestone	
Milestone		Rolled Up Milestone		External Tasks	□	Deadline	